Department of Distributed and Dependable Systems
Technical report no. D3S-TR-2020-01
October, 2020

# Reference mutability for DOT – roDOT definitions and proofs

Vlastimil Dort and Ondřej Lhoták

**Abstract:** This technical report presents the full definitions, properties and proofs for roDOT. roDOT is a version of DOT calculus based on kDOT, which adds support for reference mutability types.

This work was partially supported by the Czech Science Foundation project 18-17403S, partially supported by the Mobility Fund of Charles University, and partially supported by the Charles University institutional funding project SVV 260588. This research was supported by the Natural Sciences and Engineering Research Council of Canada.

# Contents

# 1 Introduction

This document contains full definitions and proofs for the paper Reference Immutability for DOT [1]. Section 2 shows full definition of the baseline DOT, which is a version of kDOT [3, 2] with minor modifications. Section 3 shows full definition of DOT with reference immutability. Section 4 contains further definitions which are used by proofs and lemmata.

Section 5 contains lemmata and theorems with proofs. The main theorems – Safety Theorem 5.173(S) and Immutability Guarantee 5.181(IG) are at the end, in Section 5.4. Lemmata are ordered by dependencies, so that a proof of lemma uses lemmata stated above the one being proven.

# 2 Baseline DOT Definitions

## 2.1 Baseline Syntax

The baseline syntax defines how to form types, terms and typing contexts. Compared to kDOT, the syntax for constructors is removed. Instead of a constructor, an object literal is used to create an object. The concepts of heap items and literals are merged. The baseline DOT explicitly distinguishes variables from terms. If variable $x$ is to be used as a term, it is wrapped as $\mathsf{v}x$.

| $x$ ::= | **Variable** |
|---|---|
| $\mid z$ | local |
| $\mid s$ | self |
| $\mid y$ | location |
| $d$ ::= | **Definition** |
| $\mid \{a = t\}$ | field |
| $\mid \{A = T\}$ | type |
| $\mid d_1 \wedge d_2$ | aggregate |
| $\Gamma$ ::= | **Context** |
| $\mid$ | empty |
| $\mid \Gamma, x : T$ | binding |

| $l$ ::= | **Literal** |
|---|---|
| $\mid \nu(s : T)d$ | object |
| $\mid \lambda(z : T)t$ | lambda |
| $t$ ::= | **Term** |
| $\mid \mathsf{v}x$ | var |
| $\mid \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$ | let |
| $\mid \mathsf{let}\ z = l\ \mathsf{in}\ t$ | let-lit |
| $\mid x_1.a := x_2$ | write |
| $\mid x.a$ | read |
| $\mid x_1 x_2$ | apply |

| $T$ ::= | **Type** |
|---|---|
| $\mid \top$ | top |
| $\mid \bot$ | bottom |
| $\mid \forall(z : T_1)T_2$ | function |
| $\mid \mu(s : T)$ | recursive |
| $\mid \{a : T_1..T_2\}$ | field decl |
| $\mid \{A : T_1..T_2\}$ | type decl |
| $\mid x.A$ | projection |
| $\mid T_1 \wedge T_2$ | intersection |

## 2.2 Baseline Typing

Term typing (BTT) and variable typing (BVT) defines what types a term or a variable has under a typing context. We define typing for variables and terms separately, whereas in kDOT, it is a single definition which does not distinguish variables from terms. We adjust the rules from kDOT for the removal of constructors and split rules applying to variables from rules applying to other terms. Subsumption rule exists in both typings. An additional rule (BVT-Var) allows using a variable as a term of the same type.

$$\frac{x \notin \mathrm{dom}\ \Gamma_2}{\Gamma_1, x : T, \Gamma_2 \vdash x : T}\text{(BVT-Var)}$$

$$\frac{\Gamma \vdash x : \mu(s : T)}{\Gamma \vdash x : [x/s]T}\text{(BVT-RecE)}$$

$$\frac{\Gamma \vdash x : [x/s]T}{\Gamma \vdash x : \mu(s : T)}\text{(BVT-RecI)}$$

$$\frac{\begin{array}{c}\Gamma \vdash x : T_1 \\ \Gamma \vdash x : T_2\end{array}}{\Gamma \vdash x : T_1 \wedge T_2}\text{(BVT-AndI)}$$

$$\frac{\begin{array}{c}\Gamma \vdash x : T_1 \\ \Gamma \vdash T_1 <: T_2\end{array}}{\Gamma \vdash x : T_2}\text{(BVT-Sub)}$$

$$\frac{\Gamma \vdash x : T}{\Gamma \vdash \mathsf{v}x : T}\text{(BTT-Var)}$$

$$\frac{\begin{array}{c}\Gamma \vdash x_1 : \forall(z : T_1)T_2 \\ \Gamma \vdash x_2 : T_1\end{array}}{\Gamma \vdash x_1 x_2 : [x_2/z]T_2}\text{(BTT-Apply)}$$

$$\frac{\Gamma \vdash x : \{a : T_2..T_3\}}{\Gamma \vdash x.a : T_3}\text{(BTT-Read)}$$

$$\frac{\begin{array}{c}\Gamma \vdash x_1 : T_1 \\ \Gamma \vdash x : \{a : T_1..T_2\}\end{array}}{\Gamma \vdash x.a := x_1 : T_2}\text{(BTT-Write)}$$

$$\frac{\begin{array}{c}\Gamma \vdash t : T_1 \\ \Gamma \vdash T_1 <: T_2\end{array}}{\Gamma \vdash t : T_2}\text{(BTT-Sub)}$$

$$\frac{\begin{array}{c}\Gamma, s : T_1 \vdash d : T_1 \\ \Gamma, z : T_1 \vdash t : T_2 \\ z \notin \mathrm{fv}\ T_2\end{array}}{\Gamma \vdash \mathsf{let}\ z = \nu(s : T_1)d\ \mathsf{in}\ t : T_2}\text{(BTT-New)}$$

$$\frac{\begin{array}{c}\Gamma, z_1 : T_1 \vdash t_1 : T_2 \\ \Gamma, z : T_2 \vdash t_2 : T_3 \\ z_1 \notin \mathrm{fv}\ T_1 \\ z_2 \notin \mathrm{fv}\ T_3\end{array}}{\Gamma \vdash \mathsf{let}\ z_2 = \lambda(z_1 : T_1)t_1\ \mathsf{in}\ t_2 : T_3}\text{(BTT-Fn)}$$

$$\frac{\begin{array}{c}\Gamma \vdash t_1 : T_1 \\ \Gamma, z : T_1 \vdash t_2 : T_2 \\ z \notin \mathrm{fv}\ T_2\end{array}}{\Gamma \vdash \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2 : T_2}\text{(BTT-Let)}$$

## 2.3 Baseline Definition Typing

Definition typing (BDT) is used to give types to definitions which are a part of object literals, either on the heap or in a let-lit term. It relates the field definitions and type definitions with field declaration types and type declaration types, and gives an intersection type to an aggregate of definitions.

$$\frac{}{\Gamma \vdash \{A = T\} : \{A : T..T\}}\text{(BDT-Typ)}$$

$$\frac{\Gamma \vdash t : T}{\Gamma \vdash \{a = t\} : \{a : T..T\}}\text{(BDT-Fld)}$$

$$\frac{\begin{array}{c}\Gamma \vdash d_1 : T_1\\ \Gamma \vdash d_2 : T_2\\ d_1 \text{ and } d_2 \text{ have distinct member names}\end{array}}{\Gamma \vdash d_1 \wedge d_2 : T_1 \wedge T_2}\text{(BDT-And)}$$

## 2.4 Baseline Subtyping

Subtyping in the baseline DOT is defined the same as in kDOT.

$$\frac{}{\Gamma \vdash T <: \top}\text{(BST-Top)}$$

$$\frac{}{\Gamma \vdash T_1 \wedge T_2 <: T_1}\text{(BST-And1)}$$

$$\frac{}{\Gamma \vdash \bot <: T}\text{(BST-Bot)}$$

$$\frac{}{\Gamma \vdash T_1 \wedge T_2 <: T_2}\text{(BST-And2)}$$

$$\frac{}{\Gamma \vdash T <: T}\text{(BST-Refl)}$$

$$\frac{\begin{array}{c}\Gamma \vdash T_1 <: T_2\\ \Gamma \vdash T_1 <: T_3\end{array}}{\Gamma \vdash T_1 <: T_2 \wedge T_3}\text{(BST-And)}$$

$$\frac{\begin{array}{c}\Gamma \vdash T_1 <: T_2\\ \Gamma \vdash T_2 <: T_3\end{array}}{\Gamma \vdash T_1 <: T_3}\text{(BST-Trans)}$$

$$\frac{\begin{array}{c}\Gamma \vdash T_3 <: T_1\\ \Gamma \vdash T_2 <: T_4\end{array}}{\Gamma \vdash \{A : T_1..T_2\} <: \{A : T_3..T_4\}}\text{(BST-Typ)}$$

$$\frac{\Gamma \vdash x : \{A : T_1..T_2\}}{\Gamma \vdash T_1 <: x.A}\text{(BST-SelL)}$$

$$\frac{\begin{array}{c}\Gamma \vdash T_3 <: T_1\\ \Gamma \vdash T_2 <: T_4\end{array}}{\Gamma \vdash \{a : T_1..T_2\} <: \{a : T_3..T_4\}}\text{(BST-Fld)}$$

$$\frac{\Gamma \vdash x : \{A : T_1..T_2\}}{\Gamma \vdash x.A <: T_2}\text{(BST-SelU)}$$

$$\frac{\begin{array}{c}\Gamma \vdash T_3 <: T_1\\ \Gamma, z : T_3 \vdash T_2 <: T_4\end{array}}{\Gamma \vdash \forall(z : T_1)T_2 <: \forall(z : T_3)T_4}\text{(BST-Fn)}$$

## 2.5 Baseline Runtime Syntax

We use $y \to d$ as a syntax for heap items instead of $y = d$ to avoid confusion with equality. We use the name $\sigma$ for stacks, because we use $s$ for self variables. Compared to kDOT, there is only one kind of stack frame, for evaluating let terms. The syntax of record and inert types is also defined.

| | |
|---|---|
| $\Sigma$ ::= | **Heap** |
| \| $\cdot$ | empty heap |
| \| $\Sigma, y \to l$ | heap object |
| $\sigma$ ::= | **Stack** |
| \| $\cdot$ | empty stack |
| \| let $z = \square$ in $t$ :: $\sigma$ | let frame |
| F ::= | **Inert context** |
| \| | empty |
| \| F, $y : S$ | binding |

| | |
|---|---|
| $c$ ::= | **Configuration** |
| \| $\langle t; \sigma; \Sigma\rangle$ | |
| $Q$ ::= | **Member type** |
| \| $\{a : T..T\}$ | tight field decl |
| \| $\{A : T..T\}$ | tight type decl |
| $R$ ::= | **Record type** |
| \| $Q$ | member |
| \| $R_1 \wedge R_2$ | intersection |
| $S$ ::= | **Inert type** |
| \| $\forall(z : T_1)T_2$ | function |
| \| $\mu(s : R)$ | object |

## 2.6 Baseline Inert Context

In an inert context, all variables are locations $y$, and all types are inert types ($S$). The type member declarations must be of the form $\{A : T..T\}$. The field declarations must be of the form $\{a : T..T\}$. The type of variable $y$ can only refer to variables defined previously in the context (cannot refer to following variables or $y$ itself). General contexts are denoted by Γ, inert contexts by F.

## 2.7 Baseline Reduction

The reduction relation defines operational semantics for the baseline DOT. Compared to kDOT, we remove the rules for constructors and return frames.

$$\frac{y_1 \to \nu(s : T) \ldots_1 \{a = t\} \ldots_2 \in \Sigma}{\langle y_1.a; \sigma; \Sigma\rangle \longmapsto \langle t; \sigma; \Sigma\rangle}\text{(BR-Read)}$$

$$\frac{\begin{array}{c} y_1 \to \nu(s : T) \ldots_1 \{a = t\} \ldots_2 \in \Sigma_1 \\ \Sigma_2 = \Sigma_1[y_1 \to \nu(s : T) \ldots_1 \{a = \mathsf{v}y_2\} \ldots_2] \end{array}}{\langle y_1.a := y_2; \sigma; \Sigma_1\rangle \longmapsto \langle \mathsf{v}y_2; \sigma; \Sigma_2\rangle}\text{(BR-Write)}$$

$$\frac{y_1 \to \lambda(z : T)t \in \Sigma}{\langle y_1 y_2; \sigma; \Sigma\rangle \longmapsto \langle [y_2/z]t; \sigma; \Sigma\rangle}\text{(BR-Apply)}$$

$$\frac{\Sigma_2 = \Sigma_1, y \to \lambda(z_1 : T)t_1}{\langle \mathsf{let}\ z_2 = \lambda(z_1 : T)t_1\ \mathsf{in}\ t_2; \sigma; \Sigma_1\rangle \longmapsto \langle [y/z_2]t_2; \sigma; \Sigma_2\rangle}\text{(BR-LetFn)}$$

$$\frac{\Sigma_2 = \Sigma_1, y \to \nu(s : T)[y/s]d}{\langle \mathsf{let}\ z = \nu(s : T)d\ \mathsf{in}\ t; \sigma; \Sigma_1\rangle \longmapsto \langle [y/z]t; \sigma; \Sigma_2\rangle}\text{(BR-LetNew)}$$

$$\frac{}{\langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma; \Sigma\rangle \longmapsto \langle t_1; \mathsf{let}\ z = \square\ \mathsf{in}\ t_2 :: \sigma; \Sigma\rangle}\text{(BR-LetPush)}$$

$$\frac{}{\langle \mathsf{v}y; \mathsf{let}\ z = \square\ \mathsf{in}\ t :: \sigma; \Sigma\rangle \longmapsto \langle [y/z]t; \sigma; \Sigma\rangle}\text{(BR-LetLoc)}$$

## 2.8 Baseline Configuration Typing

Configuration typing defines which configurations are valid. It relates the types of objects in the heap to the locations in the typing context, and relates the type of the term which is in the focus of exection with the type of the top frame of the stack.

$$\frac{\mathrm{F} \vdash T_1 <: T_2}{\mathrm{F} \vdash \cdot : T_1, T_2}\text{(BCT-EmptyS)}$$

$$\frac{}{\mathrm{F} \vdash \sim \cdot}\text{(BCT-EmptyH)}$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash \sigma : T_2, T_3 \\ \mathrm{F}, z : T_1 \vdash t : T_2 \\ z \notin \text{fv } T_2\end{array}}{\mathrm{F} \vdash \mathsf{let}\ z = \Box\ \mathsf{in}\ t :: \sigma : T_1, T_3}\text{(BCT-LetS)}$$

$$\frac{\begin{array}{c}\mathrm{F}_1 \vdash \mathrm{F}_2 \sim \Sigma \\ \mathrm{F}_1, z : T_1 \vdash t : T_2 \\ z \notin \text{fv } T_1\end{array}}{\mathrm{F}_1 \vdash \mathrm{F}_2, y : \forall(z : T_1)T_2 \sim \Sigma, y \to \lambda(z : T_1)t}\text{(BCT-FnH)}$$

$$\frac{\begin{array}{c}\mathrm{F}_1 \vdash \mathrm{F}_2 \sim \Sigma \\ \mathrm{F}_1 \vdash d : [y/s]R\end{array}}{\mathrm{F}_1 \vdash \mathrm{F}_2, y : \mu(s : R) \sim \Sigma, y \to \nu(s : R)d}\text{(BCT-ObjH)}$$

$$\frac{\mathrm{F} \vdash \mathrm{F} \sim \Sigma}{\mathrm{F} \sim \Sigma}\text{(BCT-CorrH)} \qquad \frac{\begin{array}{c}\mathrm{F} \sim \Sigma \\ \mathrm{F} \vdash t : T_1 \\ \mathrm{F} \vdash \sigma : T_1, T_2\end{array}}{\mathrm{F} \vdash \langle t; \sigma; \Sigma \rangle : T_2}\text{(BCT-Corr)}$$

# 3 roDOT Definitions

## 3.1 Syntax

Programs are represented by terms in ANF. A let-lit term at runtime creates an object with members specified by a definition $d$, which can contain field, method and type members. Correctly formed terms are typed under a typing context $\Gamma$.

| | | | |
|---|---|---|---|
| $x ::=$ | **Variable** | $\Gamma ::=$ | **Context** |
| $\mid u$ | abstract | $\mid$ | empty |
| $\mid v$ | global | $\mid \Gamma, x : T$ | binding |
| $u ::=$ | **Abstract** | $\mid \Gamma, !$ | hide |
| $\mid z$ | local | $d ::=$ | **Definition** |
| $\mid s$ | self | $\mid \{a = x\}$ | field |
| $\mid r$ | receiver | $\mid \{m(z, r) = t\}$ | method |
| $v ::=$ | **Global** | $\mid \{A(r) = T\}$ | type |
| $\mid y$ | location | $\mid d_1 \wedge d_2$ | aggregate |
| $\mid w$ | reference | $T ::=$ | **Type** |
| $t ::=$ | **Term** | $\mid \top$ | top |
| $\mid \mathsf{v}x$ | var | $\mid \bot$ | bottom |
| $\mid \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$ | let | $\mid \mu(s : T)$ | recursive |
| $\mid \mathsf{let}\ z = \nu(s : T)d\ \mathsf{in}\ t$ | let-lit | $\mid \{a : T_1..T_2\}$ | field decl |
| $\mid x_1.a := x_2$ | write | $\mid \{m(z : T_1, r : T_3) : T_2\}$ | method decl |
| $\mid x.a$ | read | $\mid \{B(r) : T_1..T_2\}$ | type decl |
| $\mid x_1.m\, x_2$ | call | $\mid x_1.B(x_2)$ | projection |
| $B ::=$ | **Type name** | $\mid T_1 \wedge T_2$ | intersection |
| $\mid A$ | type member | $\mid T_1 \vee T_2$ | union |
| $\mid \mathsf{M}$ | mutability | $\mid \mathsf{N}$ | read-only bottom |

### 3.1.1 Receiver Parameter

The problem is, that we want to refer to the mutability of the receiver in the return types of methods (it is required to precisely describe mutability of field read). However, if we use $s.\mathsf{M}$ for that purpose, for example $\Gamma;\rho \vdash \{m(z) = s\} : \{m(z : \top) : \{\mathsf{M} : s.\mathsf{M}\}\}$, then the type of a mutable value $\Gamma;\rho \vdash y : \mu(s : \{m(z : T) : \{\mathsf{M} : s.\mathsf{M}\}\})$ can be opened to $\Gamma;\rho \vdash y : \{m(z : T) : \{\mathsf{M} : y.\mathsf{M}\}\}$, which is a subtype of $\Gamma;\rho \vdash y : \{m(z : T) : \{\mathsf{M} : \bot\}\}$. This value can be stored to a field $a$ of type $\{m(z : T) : \{\mathsf{M} : \bot\}\}$, which is considered to be a read-only field. Also, when reading this field from a read-only reference, viewpoint adaptation does not affect its type. Therefore, unless there are other paths to $y$, $y$ should not be mutably reachable through the field $a$. However, at the same time, we can use the value of this field to call $m$, which returns a mutable reference to $y$.

The solution is to forbid the mutability of a value from being propagated into the types of its methods. That is done by disallowing $s.\mathsf{M}$ in the declaration types. Instead, we introduce a variable $r$ bound in the method type, and refer to the mutability of the receiver by $r.\mathsf{M}$. We could also use a type variable, but that would require more syntax extensions: type variables and subtyping bounds in the typing context.

To allow giving name to return types containing $r.\mathsf{M}$, there must be a way to use $r.\mathsf{M}$ in the definitions of type members. That means adding a parameter $r$ to type members. For simplicity, we add a parameter to every type member and don't allow bounds. Even the special $\mathsf{M}$ type member has such parameter, but it has no use. Also, every type selection $x_1.B(x_2)$ needs to specify an argument.

The consequence is, that for $w \to y \in \rho$, for normal type members, $y.A(x_2)$ is equivalent $w.A(x_2)$ (subtyping in both directions). For mutability type member, just one direction: $\Gamma;\rho \vdash y.\mathsf{M}(x_2) <: w.\mathsf{M}(x_2)$.

### 3.1.2 Kinds of Variables

There are five basic kinds of variables: $z$ for method parameters and local variables. $r$ for receiver parameters of methods and type memebers. $s$ for self reference of objects. $y$ for heap locations. $w$ for object references. The letter $x$ can be any of those. The letter $u$ can be $z$, $s$ or $r$. In initial configurations, there can only be $z$, $r$ and $s$. They must be bound. In domains of inert contexts, there can only be $y$ or $w$.

In domains of heaps and values of fields on a heap, there can only be $y$. Free variables in terms during typed reduction can be $w$. In domain of general context, there can be $y$, $w$, $z$, $r$ and $s$. In prefix of type selection, there can be $y$, $w$, $z$, $r$ and $s$. In a context for definition typing, there is always $s$ at the end. In a context for a method body, variables in the context are hidden, except $r$ and $z$ at the end.

### 3.1.3 Alpha Equivalence

We assume alpha-equialent terms, types, statements, and other structures, to be equal. We assume that in every context, variable names are distinct. Therefore, whenever we write $\Gamma = \Gamma_1, x : T, \Gamma_2$, then we can assume that $x \notin \text{dom}\,\Gamma_1$ and $x \notin \text{dom}\,\Gamma_2$. Examples of alpha equivalence (not exhaustive):

$$\begin{gathered}
\mu(s_1 : T) = \mu(s_2 : [s_2/s_1]T) \\
\nu(s_1 : T)d = \nu(s_2 : [s_2/s_1]T)[s_2/s_1]d \\
\{m(z_1 : T_1, r_1 : T_3) : T_2\} = \{m(z_2 : [z_2/z_1]T_1, r_2 : [r_2/r_1][z_2/z_1]T_3) : [r_2/r_1][z_2/z_1]T_2\} \\
\{m(z_1, r_1) = t\} = \{m(z_2, r_2) = [r_2/r_1][z_2/z_1]t\} \\
\Gamma_1, x_1 : T_1, \Gamma_2 ; \rho \vdash x_3 : T_3 = \Gamma_1, x_1 : [x_2/x_1]T_1, [x_2/x_1]\Gamma_2 ; [x_2/x_1]\rho \vdash [x_2/x_1]x_3 : [x_2/x_1]T_3
\end{gathered}$$

## 3.2 Substitution

*Substitution* $[x_2/x_1]X$ replaces all free occurences of $x_1$ in $X$ by $x_2$, where $X$ can be a variable $x_3$, a term $t$, a definition $d$ or a type $T$. A variable also can be substituted in a suffix of a typing context. Substitution lemmata are stated in Section 5.1.5.

$$\frac{}{[x_2/x_1]x_1 = x_2}\,(\text{VX-VarE})$$

$$\frac{x_3 \neq x_1}{[x_2/x_1]x_3 = x_3}\,(\text{VX-VarN})$$

$$\frac{}{[x_2/x_1]\mathsf{v}x_3 = \mathsf{v}[x_2/x_1]x_3}\,(\text{EX-Var})$$

$$\frac{}{[x_2/x_1]x_3.a = [x_2/x_1]x_3.a}\,(\text{EX-Read})$$

$$\frac{}{[x_2/x_1]x_3.a := x_4 = [x_2/x_1]x_3.a := [x_2/x_1]x_4}\,(\text{EX-Write})$$

$$\frac{}{[x_2/x_1]x_3.m\,x_4 = [x_2/x_1]x_3.m\,[x_2/x_1]x_4}\,(\text{EX-Apply})$$

$$\frac{}{[x_2/x_1]\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2 = \mathsf{let}\ z = [x_2/x_1]t_1\ \mathsf{in}\ [x_2/x_1]t_2}\,(\text{EX-Let})$$

$$\frac{t = \mathsf{let}\ z = \nu(s : T)d\ \mathsf{in}\ t_2}{[x_2/x_1]t = \mathsf{let}\ z = \nu(s : [x_2/x_1]T)[x_2/x_1]d\ \mathsf{in}\ [x_2/x_1]t_2}\,(\text{EX-LetNew})$$

$$\frac{}{[x_2/x_1]\{a = x_3\} = \{a = [x_2/x_1]x_3\}}\,(\text{DX-Fld})$$

$$\frac{}{[x_2/x_1]\{A(r) = T\} = \{A(r) = [x_2/x_1]T\}}\,(\text{DX-Typ})$$

$$\frac{}{[x_2/x_1]\{m(z, r) = t\} = \{m(z, r) = [x_2/x_1]t\}}\,(\text{DX-Met})$$

$$\frac{}{[x_2/x_1]d_1 \wedge d_2 = [x_2/x_1]d_1 \wedge [x_2/x_1]d_2}\,(\text{DX-And})$$

$$\frac{}{[x_2/x_1]\top = \top}\text{(TX-Top)}$$

$$\frac{}{[x_2/x_1]\bot = \bot}\text{(TX-Bot)}$$

$$\frac{}{[x_2/x_1]\mathsf{N} = \mathsf{N}}\text{(TX-N)}$$

$$\frac{}{[x_2/x_1]T_1 \land T_2 = [x_2/x_1]T_1 \land [x_2/x_1]T_2}\text{(TX-And)}$$

$$\frac{}{[x_2/x_1]T_1 \lor T_2 = [x_2/x_1]T_1 \lor [x_2/x_1]T_2}\text{(TX-Or)}$$

$$\frac{x_1 \neq s \land x_2 \neq s}{[x_2/x_1]\mu(s : T_1) = \mu(s : [x_2/x_1]T_1)}\text{(TX-Rec)}$$

$$\frac{}{[x_2/x_1]\{a : T_1..T_2\} = \{a : [x_2/x_1]T_1..[x_2/x_1]T_2\}}\text{(TX-Fld)}$$

$$\frac{x_1 \neq r \land x_2 \neq r}{[x_2/x_1]\{A(r) : T_1..T_2\} = \{A(r) : [x_2/x_1]T_1..[x_2/x_1]T_2\}}\text{(TX-Typ)}$$

$$\frac{\begin{array}{c} T = \{m(z : T_1, r : T_2) : T_3\} \\ x_1 \neq z \land x_2 \neq z \land x_1 \neq r \land x_2 \neq r \end{array}}{[x_2/x_1]T = \{m(z : [x_2/x_1]T_1, r : [x_2/x_1]T_2) : [x_2/x_1]T_3\}}\text{(TX-Met)}$$

$$\frac{}{[x_2/x_1]x_3.B(x_4) = [x_2/x_1]x_3.B([x_2/x_1]x_4)}\text{(TX-Sel)}$$

$$\frac{}{[x_2/x_1]\Gamma, x_3 : T_1 = [x_2/x_1]\Gamma, [x_2/x_1]x_3 : [x_2/x_1]T_1}\text{(CX-Bind)}$$

## 3.3 Ellipsis

Definition $d$ of an object is written as an intersection of individual field, method and type member definitions. To say that a definition $d_1$ is a part of definition $d_2$, we write $d_2 = \ldots_1 d_1 \ldots_2$. Similarly, we write $T_2 = \ldots_1 T_1 \ldots_2$ for the corresponding declaration types.

$$\frac{\begin{array}{c} \ldots_1 = \cdot \\ \ldots_2 = \cdot \end{array}}{d = \ldots_1 d \ldots_2}\text{(DL-Refl)} \qquad \frac{\begin{array}{c} \ldots_1 = \cdot \\ \ldots_2 = \cdot \end{array}}{T = \ldots_1 T \ldots_2}\text{(TL-Refl)}$$

$$\frac{\begin{array}{c} d_1 = \ldots_1 d_3 \ldots_2 \\ \ldots_3 = \ldots_2 , d_2 \end{array}}{d_1 \land d_2 = \ldots_1 d_3 \ldots_3}\text{(DL-And1)} \qquad \frac{\begin{array}{c} T_1 = \ldots_1 T_3 \ldots_2 \\ \ldots_3 = \ldots_2 , T_2 \end{array}}{T_1 \land T_2 = \ldots_1 T_3 \ldots_3}\text{(TL-And1)}$$

$$\frac{\begin{array}{c} d_2 = \ldots_1 d_3 \ldots_2 \\ \ldots_3 = d_1, \ldots_1 \end{array}}{d_1 \land d_2 = \ldots_3 d_3 \ldots_2}\text{(DL-And2)} \qquad \frac{\begin{array}{c} T_2 = \ldots_1 T_3 \ldots_2 \\ \ldots_3 = T_1, \ldots_1 \end{array}}{T_1 \land T_2 = \ldots_3 T_3 \ldots_2}\text{(TL-And2)}$$

## 3.4 Independence

The *independence* relation $T$ $\mathbf{indep}$ $s$ states that a type $T$ is independent on a variable $s$, meaning that the type $T$ does not select the mutability member $\mathsf{M}$ on $s$. Could be equivalently defined as $\forall r_0 \colon s.\mathsf{M}(r_0) \notin T$ and $\forall x, B \colon x.B(s) \notin T$.

$$\frac{}{\top\ \mathbf{indep}\ s}\text{(TI-Top)}$$

$$\frac{}{\bot\ \mathbf{indep}\ s}\text{(TI-Bot)}$$

$$\frac{}{\mathsf{N}\ \mathbf{indep}\ s}\text{(TI-N)}$$

$$\frac{\begin{array}{c}T_1\ \mathbf{indep}\ s\\ T_2\ \mathbf{indep}\ s\end{array}}{T_1 \wedge T_2\ \mathbf{indep}\ s}\text{(TI-And)}$$

$$\frac{\begin{array}{c}T_1\ \mathbf{indep}\ s\\ T_2\ \mathbf{indep}\ s\end{array}}{T_1 \vee T_2\ \mathbf{indep}\ s}\text{(TI-Or)}$$

$$\frac{\begin{array}{c}x \neq s\\ x_2 \neq s\end{array}}{x.\mathsf{M}(x_2)\ \mathbf{indep}\ s}\text{(TI-SelM)}$$

$$\frac{x_2 \neq s}{x.A(x_2)\ \mathbf{indep}\ s}\text{(TI-SelA)}$$

$$\frac{T\ \mathbf{indep}\ s}{\mu(s_2 : T)\ \mathbf{indep}\ s}\text{(TI-Rec)}$$

$$\frac{\begin{array}{c}T_1\ \mathbf{indep}\ s\\ T_2\ \mathbf{indep}\ s\end{array}}{\{A(r) : T_1..T_2\}\ \mathbf{indep}\ s}\text{(TI-Typ)}$$

$$\frac{\begin{array}{c}T_1\ \mathbf{indep}\ s\\ T_2\ \mathbf{indep}\ s\end{array}}{\{a : T_1..T_2\}\ \mathbf{indep}\ s}\text{(TI-Fld)}$$

$$\frac{\begin{array}{c}T_1\ \mathbf{indep}\ s\\ T_2\ \mathbf{indep}\ s\\ T_3\ \mathbf{indep}\ s\end{array}}{\{m(z : T_1, r : T_3) : T_2\}\ \mathbf{indep}\ s}\text{(TI-Met)}$$

## 3.5 Dereferencing

The *dereference* substitution $[\rho]d$ replaces reference variables in $d$ by the corresponding location variables from $\rho$. This is used in the (R-LetNew) reduction rule to ensure that values of fields on the heap are always heap locations.

$$\frac{w \to y \in \rho}{[\rho]w = y}\text{(DU-Var)}$$

$$\frac{x \notin \text{dom}\ \rho}{[\rho]x = x}\text{(DU-VarN)}$$

$$\frac{}{[\rho]\{a = x\} = \{a = [\rho]x\}}\text{(DU-Fld)}$$

$$\frac{}{[\rho]\{B(r) = T\} = \{B(r) = T\}}\text{(DU-Typ)}$$

$$\frac{}{[\rho]\{m(z, r) = t\} = \{m(z, r) = t\}}\text{(DU-Met)}$$

$$\frac{}{[\rho]d_1 \wedge d_2 = [\rho]d_1 \wedge [\rho]d_2}\text{(DU-And)}$$

## 3.6 Typing

The *typing* relations $\Gamma;\rho \vdash x : T$ and $\Gamma;\rho \vdash t : T$ mean that the variable $x$ or a term $t$ has the type $T$ in the typing context $\Gamma$ and the environment $\rho$.

$$\frac{! \notin \Gamma_2}{\Gamma_1, x : T, \Gamma_2 \ \mathbf{vis}\ x}\text{(Vis-Var)}$$

$$\frac{\Gamma = \Gamma_1, x : T, \Gamma_2}{\Gamma;\rho \vdash x : T}\text{(VT-Var)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : T_1\\ \Gamma;\rho \vdash T_1 <: T_2\end{array}}{\Gamma;\rho \vdash x : T_2}\text{(VT-Sub)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : T_1\\ \Gamma;\rho \vdash x : T_2\end{array}}{\Gamma;\rho \vdash x : T_1 \wedge T_2}\text{(VT-AndI)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : T\\ \Gamma\ \mathbf{vis}\ x\end{array}}{\Gamma;\rho \vdash \mathsf{v}x : T}\text{(TT-Var)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash t : T_1\\ \Gamma;\rho \vdash T_1 <: T_2\end{array}}{\Gamma;\rho \vdash t : T_2}\text{(TT-Sub)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash t_1 : T_1\\ \Gamma, z : T_1;\rho \vdash t_2 : T_2\\ z \notin \mathrm{fv}\ T_2\end{array}}{\Gamma;\rho \vdash \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2 : T_2}\text{(TT-Let)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : \mu(s : T)\\ T\ \mathbf{indep}\ s\end{array}}{\Gamma;\rho \vdash x : [x/s]T}\text{(VT-RecE)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : [x/s]T\\ T\ \mathbf{indep}\ s\\ \Gamma;\rho \vdash [x/s]T\ \mathbf{ro}\ [x/s]T\end{array}}{\Gamma;\rho \vdash x : \mu(s : T)}\text{(VT-RecI)}$$

$$\frac{\Gamma;\rho \vdash x : T}{\Gamma;\rho \vdash x : \{\mathsf{M}(r_0) : \bot..\top\}}\text{(VT-MutTop)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x_1 : \{m(z : T_1, r : T_3) : T_2\}\\ \Gamma;\rho \vdash x_1 : [x_2/z]T_3\\ \Gamma;\rho \vdash x_2 : T_1\\ \Gamma\ \mathbf{vis}\ x_1 \qquad \Gamma\ \mathbf{vis}\ x_2\end{array}}{\Gamma;\rho \vdash x_1.m\, x_2 : [x_1/r][x_2/z]T_2}\text{(TT-Apply)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x_1 : T_1\\ \Gamma;\rho \vdash x : \{a : T_1..T_2\}\\ \Gamma;\rho \vdash x : \{\mathsf{M}(r_0) : \bot..\bot\}\\ \Gamma\ \mathbf{vis}\ x_1 \qquad \Gamma\ \mathbf{vis}\ x\end{array}}{\Gamma;\rho \vdash x.a := x_1 : T_2}\text{(TT-Write)}$$

$$\frac{\begin{array}{c}\Gamma, s : T_1;\rho \vdash d : T_1\\ \Gamma, z : \mu(s : T_1) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash t : T_2\\ z \notin \mathrm{fv}\ T_2\\ T_1\ \mathbf{indep}\ s\end{array}}{\Gamma;\rho \vdash \mathsf{let}\ z = \nu(s : T_1)d\ \mathsf{in}\ t : T_2}\text{(TT-New)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : \{a : T_1..T_2\}\\ \Gamma;\rho \vdash T_2\ \mathbf{ro}\ T_3\\ \Gamma;\rho \vdash T_2\ \mathbf{mu}(r)\ T_4\\ \Gamma\ \mathbf{vis}\ x\end{array}}{\Gamma;\rho \vdash x.a : T_3 \wedge \{\mathsf{M}(r) : \bot..(T_4 \vee x.\mathsf{M}(r))\}}\text{(TT-Read)}$$

## 3.7 Definition Typing

The typing relation for definitions $\Gamma, s : T_4;\rho \vdash d : T$. mean that the definition $d$ has the type $T$ in the typing context Γ, where the self-variable $s$ of the object being defined has type $T_4$. There is a cyclic dependency between term typing and method typing, through (DT-Met) and (TT-New).

$$\frac{}{\Gamma, s : T_4;\rho \vdash \{A(r) = T\} : \{A(r) : T..T\}}\text{(DT-Typ)}$$

$$\frac{}{\Gamma, s : T_4;\rho \vdash \{A(r) = T\} : \{A(r) : \bot..T\}}\text{(DT-TypB)}$$

$$\frac{\begin{array}{c}\Gamma, s : T_4;\rho \vdash x : T\\ \Gamma, s : T_4 \textbf{ vis } x\end{array}}{\Gamma, s : T_4;\rho \vdash \{a = x\} : \{a : T..T\}}\text{(DT-Fld)}$$

$$\frac{\begin{array}{c}\Gamma, s : T_4;\rho \vdash d_1 : T_1\\ \Gamma, s : T_4;\rho \vdash d_2 : T_2\\ d_1 \text{ and } d_2 \text{ have distinct member names}\end{array}}{\Gamma, s : T_4;\rho \vdash d_1 \wedge d_2 : T_1 \wedge T_2}\text{(DT-And)}$$

$$\frac{\begin{array}{c}z \notin \text{fv } T_1 \cup \text{fv } T_4, r \notin \text{fv } T_3 \cup \text{fv } T_1 \cup \text{fv } T_4\\ \Gamma, s : T_4, !, z : T_1, r : T_4 \wedge [r/s]T_4 \wedge T_3;\rho \vdash t : T_2\end{array}}{\Gamma, s : T_4;\rho \vdash \{m(z, r) = t\} : \{m(z : T_1, r : T_3) : T_2\}}\text{(DT-Met)}$$

## 3.8 Heap Definition Typing

The typing relation for heap object definitions $\Gamma, y/s : R;\rho \vdash d : T$. mean that the definition $d$ has the type $T$ in the typing context $\Gamma$, where the self-variable $s$ of the object at location $y$ has type $R$ and definition $d$. It is used from the (CT-ObjH) rule of heap correspondence. Heap definition typing is distinguished from definition typing by the heap typing context $\Gamma, y/s : R$. This context ends with a triple stating that the variable $s$ with type $R$ was replaced by the location $y$ in the definition being typed. This triple is needed to construct the type given to $r$ for typing bodies of methods. The rules are similar to the corresponding definition typing rules, except that in (HT-Met) for typing method bodies, $r$ has a different type, and in (HT-Fld) and (HT-Met), $s$ is not added to the context for typing field values and method bodies.

$$\frac{}{\Gamma, y/s : T_4;\rho \vdash \{A(r) = T\} : \{A(r) : T..T\}}\text{(HT-Typ)}$$

$$\frac{}{\Gamma, y/s : T_4;\rho \vdash \{A(r) = T\} : \{A(r) : \bot..T\}}\text{(HT-TypB)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : T\\ \Gamma \textbf{ vis } x\end{array}}{\Gamma, y/s : T_4;\rho \vdash \{a = x\} : \{a : T..T\}}\text{(HT-Fld)}$$

$$\frac{\begin{array}{c}\Gamma, y/s : T_4;\rho \vdash d_1 : T_1\\ \Gamma, y/s : T_4;\rho \vdash d_2 : T_2\\ d_1 \text{ and } d_2 \text{ have distinct member names}\end{array}}{\Gamma, y/s : T_4;\rho \vdash d_1 \wedge d_2 : T_1 \wedge T_2}\text{(HT-And)}$$

$$\frac{\begin{array}{c}z \notin \text{fv } T_1 \cup \text{fv } T_4, r \notin \text{fv } T_3 \cup \text{fv } T_1 \cup \text{fv } T_4\\ \Gamma, !, z : T_1, r : [y/s]T_4 \wedge [r/s]T_4 \wedge T_3;\rho \vdash t : T_2\end{array}}{\Gamma, y/s : T_4;\rho \vdash \{m(z, r) = t\} : \{m(z : T_1, r : T_3) : T_2\}}\text{(HT-Met)}$$

## 3.9 Subtyping

The *subtyping* relation $\Gamma;\rho \vdash T_1 <: T_2$ means that the type $T_1$ is a subtype of $T_2$ in the typing context $\Gamma$ and the environment $\rho$. The typing context $\Gamma$ is used in the (ST-SelL) and (ST-SelU) rules. There is a cyclic dependency between variable typing and subtyping, through (ST-SelL) or (ST-SelU) and (VT-Sub). The environment $\rho$ is used in the (ST-Eq) rule. Useful simple properties of subtyping are stated in Section 5.1.4.

$$\frac{}{\Gamma;\rho \vdash T <: T}\text{(ST-Refl)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_1 <: T_2\\ \Gamma;\rho \vdash T_2 <: T_3\end{array}}{\Gamma;\rho \vdash T_1 <: T_3}\text{(ST-Trans)}$$

$$\frac{}{\Gamma;\rho \vdash T <: \top}\text{(ST-Top)}$$

$$\frac{}{\Gamma;\rho \vdash \bot <: T}\text{(ST-Bot)}$$

$$\frac{\rho \vdash T_1 \approx T_2}{\Gamma;\rho \vdash T_1 <: T_2}\text{(ST-Eq)}$$

$$\frac{}{\Gamma;\rho \vdash T_1 <: T_1 \vee T_2}\text{(ST-Or1)}$$

$$\frac{}{\Gamma;\rho \vdash T_2 <: T_1 \vee T_2}\text{(ST-Or2)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_1 <: T_3\\ \Gamma;\rho \vdash T_2 <: T_3\end{array}}{\Gamma;\rho \vdash T_1 \vee T_2 <: T_3}\text{(ST-Or)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_1 <: T_2\\ \Gamma;\rho \vdash T_1 <: T_3\end{array}}{\Gamma;\rho \vdash T_1 <: T_2 \wedge T_3}\text{(ST-And)}$$

$$\frac{}{\Gamma;\rho \vdash T_1 \wedge T_2 <: T_1}\text{(ST-And1)}$$

$$\frac{}{\Gamma;\rho \vdash T_1 \wedge T_2 <: T_2}\text{(ST-And2)}$$

$$\frac{\Gamma;\rho \vdash x : \{B(r) : T_1..T_2\}}{\Gamma;\rho \vdash [x_2/r]T_1 <: x.B(x_2)}\text{(ST-SelL)}$$

$$\frac{\Gamma;\rho \vdash x : \{B(r) : T_1..T_2\}}{\Gamma;\rho \vdash x.B(x_2) <: [x_2/r]T_2}\text{(ST-SelU)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_3 <: T_1\\ \Gamma;\rho \vdash T_2 <: T_4\end{array}}{\Gamma;\rho \vdash \{B(r) : T_1..T_2\} <: \{B(r) : T_3..T_4\}}\text{(ST-Typ)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_3 <: T_1\\ \Gamma;\rho \vdash T_2 <: T_4\end{array}}{\Gamma;\rho \vdash \{a : T_1..T_2\} <: \{a : T_3..T_4\}}\text{(ST-Fld)}$$

$$\frac{}{\Gamma;\rho \vdash \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: \bot}\text{(ST-N-M)}$$

$$\frac{}{\Gamma;\rho \vdash \mathsf{N} <: \mu(s : T)}\text{(ST-N-Rec)}$$

$$\frac{}{\Gamma;\rho \vdash \mathsf{N} <: \{a : T_1..T_2\}}\text{(ST-N-Fld)}$$

$$\frac{}{\Gamma;\rho \vdash \mathsf{N} <: \{A(r) : T_1..T_2\}}\text{(ST-N-Typ)}$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_3 <: T_1\\ \Gamma, z : T_3;\rho \vdash T_6 <: T_5\\ \Gamma, z : T_3, r : T_6;\rho \vdash T_2 <: T_4\end{array}}{\Gamma;\rho \vdash \{m(z : T_1, r : T_5) : T_2\} <: \{m(z : T_3, r : T_6) : T_4\}}\text{(ST-Met)}$$

$$\frac{}{\Gamma;\rho \vdash \mathsf{N} <: \{m(z : T_1, r : T_3) : T_2\}}\text{(ST-N-Met)}$$

$$\frac{}{\Gamma;\rho \vdash \{B(r) : T_1..T_2\} \wedge \{B(r) : T_3..T_4\} <: \{B(r) : T_1 \vee T_3..T_2 \wedge T_4\}}\text{(ST-TypAnd)}$$

$$\frac{}{\Gamma;\rho \vdash T_1 \wedge (T_2 \vee T_3) <: (T_1 \wedge T_2) \vee (T_1 \wedge T_3)}\text{(ST-Dist)}$$

## 3.10 Splitting

The *splitting* relations $\Gamma;\rho \vdash T_1\ \mathbf{ro}\ T_2$ and $\Gamma;\rho \vdash T_1\ \mathbf{mu}(r)\ T_3$ mean that the type $T_1$ has a read-only variant $T_2$ and mutability $T_3$ in the typing context $\Gamma$ and the environment $\rho$. The mutability can depend on the receiver variable $r$. Properties of splitting are stated in Section 5.1.6.

$$\frac{}{\begin{array}{c}\Gamma;\rho \vdash \top\ \mathbf{ro}\ \top\\ \Gamma;\rho \vdash \top\ \mathbf{mu}(r)\ \top\end{array}}\ (\text{TS-Top})$$

$$\frac{}{\begin{array}{c}\Gamma;\rho \vdash \bot\ \mathbf{ro}\ \mathsf{N}\\ \Gamma;\rho \vdash \bot\ \mathbf{mu}(r)\ \bot\end{array}}\ (\text{TS-Bot})$$

$$\frac{T = \{A(r) : T_1..T_2\}}{\begin{array}{c}\Gamma;\rho \vdash T\ \mathbf{ro}\ T\\ \Gamma;\rho \vdash T\ \mathbf{mu}(r_0)\ \top\end{array}}\ (\text{TS-Typ})$$

$$\frac{T = \{m(z : T_1, r : T_3) : T_2\}}{\begin{array}{c}\Gamma;\rho \vdash T\ \mathbf{ro}\ T\\ \Gamma;\rho \vdash T\ \mathbf{mu}(r_0)\ \top\end{array}}\ (\text{TS-Met})$$

$$\frac{T = \{a : T_1..T_2\}}{\begin{array}{c}\Gamma;\rho \vdash T\ \mathbf{ro}\ T\\ \Gamma;\rho \vdash T\ \mathbf{mu}(r)\ \top\end{array}}\ (\text{TS-Fld})$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash x : \{B(r) : T_1..T_2\}\\ \Gamma;\rho \vdash [x_2/r]T_2\ \mathbf{ro}\ T_3\\ \Gamma;\rho \vdash [x_2/r]T_2\ \mathbf{mu}(r_0)\ T_4\end{array}}{\begin{array}{c}\Gamma;\rho \vdash x.B(x_2)\ \mathbf{ro}\ T_3\\ \Gamma;\rho \vdash x.B(x_2)\ \mathbf{mu}(r_0)\ T_4\end{array}}\ (\text{TS-Sel})$$

$$\frac{}{\begin{array}{c}\Gamma;\rho \vdash \{\mathsf{M}(r) : T_1..T_2\}\ \mathbf{ro}\ \top\\ \Gamma;\rho \vdash \{\mathsf{M}(r) : T_1..T_2\}\ \mathbf{mu}(r)\ T_2\end{array}}\ (\text{TS-M})$$

$$\frac{T = \mu(s : T_1)}{\begin{array}{c}\Gamma;\rho \vdash T\ \mathbf{ro}\ T\\ \Gamma;\rho \vdash T\ \mathbf{mu}(r)\ \top\end{array}}\ (\text{TS-Rec})$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_1\ \mathbf{ro}\ T_2\\ \Gamma;\rho \vdash T_3\ \mathbf{ro}\ T_4\end{array}}{\Gamma;\rho \vdash T_1 \wedge T_3\ \mathbf{ro}\ T_2 \wedge T_4}\ (\text{TS-AndR})$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_1\ \mathbf{mu}(r)\ T_2\\ \Gamma;\rho \vdash T_3\ \mathbf{mu}(r)\ T_4\end{array}}{\Gamma;\rho \vdash T_1 \wedge T_3\ \mathbf{mu}(r)\ T_2 \wedge T_4}\ (\text{TS-AndM})$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_1\ \mathbf{ro}\ T_2\\ \Gamma;\rho \vdash T_3\ \mathbf{ro}\ T_4\end{array}}{\Gamma;\rho \vdash T_1 \vee T_3\ \mathbf{ro}\ T_2 \vee T_4}\ (\text{TS-OrR})$$

$$\frac{\begin{array}{c}\Gamma;\rho \vdash T_1\ \mathbf{mu}(r)\ T_2\\ \Gamma;\rho \vdash T_3\ \mathbf{mu}(r)\ T_4\end{array}}{\Gamma;\rho \vdash T_1 \vee T_3\ \mathbf{mu}(r)\ T_2 \vee T_4}\ (\text{TS-OrM})$$

## 3.11 Equivalence

The *equivalence* relation $\rho \vdash T_1 \approx T_2$ means that the type $T_1$ is equivalent to $T_2$ in the environment $\rho$. Two types are equivalent if the have the same structure, but they can differ in references and locations on left side of normal type selections, as long as the references correspond to the same location in $\rho$. Type selections $x_1.\mathsf{M}(x_2)$ must be the same. For example, $w \to y \vdash w.A(x) \approx y.A(x)$. Equivalence implies subtyping in both directions. The relation is reflexive, symmetric and transitive. Useful simple properties of equivalence are stated in Section 5.1.1.

$$\frac{v_1 \to v_2 \in \rho}{\rho \vdash v_1 \approx v_2}\ (\text{VE-RtoL}) \qquad \frac{}{\rho \vdash v_1 \approx v_1}\ (\text{VE-Refl})$$

$$\frac{\rho \vdash v_1 \approx v_2}{\rho \vdash v_2 \approx v_1}\ (\text{VE-Symm}) \qquad \frac{\begin{array}{c}\rho \vdash v_1 \approx v_2\\ \rho \vdash v_2 \approx v_3\end{array}}{\rho \vdash v_1 \approx v_3}\ (\text{VE-Trans})$$

$$\frac{}{\rho \vdash T \approx T}\text{(TE-Refl)}$$

$$\frac{\rho \vdash x_1 \approx x_2}{\rho \vdash x_1.A(x) \approx x_2.A(x)}\text{(TE-Sel)}$$

$$\frac{\rho \vdash T_1 \approx T_3 \quad \rho \vdash T_2 \approx T_4}{\rho \vdash T_1 \wedge T_2 \approx T_3 \wedge T_4}\text{(TE-And)}$$

$$\frac{\rho \vdash T_1 \approx T_3 \quad \rho \vdash T_2 \approx T_4}{\rho \vdash T_1 \vee T_2 \approx T_3 \vee T_4}\text{(TE-Or)}$$

$$\frac{\rho \vdash T_1 \approx T_2}{\rho \vdash \mu(s : T_1) \approx \mu(s : T_2)}\text{(TE-Rec)}$$

$$\frac{\rho \vdash T_1 \approx T_3 \quad \rho \vdash T_2 \approx T_4}{\rho \vdash \{B(r) : T_1..T_2\} \approx \{B(r) : T_3..T_4\}}\text{(TE-Typ)}$$

$$\frac{\rho \vdash T_1 \approx T_3 \quad \rho \vdash T_2 \approx T_4}{\rho \vdash \{a : T_1..T_2\} \approx \{a : T_3..T_4\}}\text{(TE-Fld)}$$

$$\frac{\rho \vdash T_1 \approx T_4 \quad \rho \vdash T_2 \approx T_5 \quad \rho \vdash T_3 \approx T_6}{\rho \vdash \{m(z : T_1, r : T_3) : T_2\} \approx \{a(z : T_4, r : T_6) : T_5\}}\text{(TE-Met)}$$

## 3.12 Runtime

A machine *configuration* is a tuple with four parts: the *focus of execution* $t$, stack $\sigma$, environment $\rho$ and heap $\Sigma$. The focus of execution $t$ is a term which decides which next step will be taken. The stack $\sigma$ contains *stack frames*, which store the second parts of let expressions during reduction of the first part. The environment $\rho$ stores the correspondence references used in terms to locations used in the heap. It maps a reference to the corresponding location. The heap $\Sigma$ stores objects. It maps locations to definitions of members of the object. Correctly formed configurations can be during execution typed in an *inert context*.

| | | | |
|---|---|---|---|
| $\Sigma ::=$ | **Heap** | $Q ::=$ | **Member type** |
| $\mid \cdot$ | empty heap | $\mid \{a : T..T\}$ | tight field |
| $\mid \Sigma, y \to d$ | heap object | $\mid \{m(z : T_1, r : T_3) : T_2\}$ | method |
| $\sigma ::=$ | **Stack** | $\mid \{A(r) : T..T\}$ | tight type |
| $\mid \cdot$ | empty stack | $\mid \{A(r) : \bot..T\}$ | upper-bounded type |
| $\mid \mathsf{let}\ z = \square\ \mathsf{in}\ t :: \sigma$ | let frame | $R ::=$ | **Record type** |
| $\rho ::=$ | **Environment** | $\mid Q$ | member |
| $\mid \cdot$ | empty environment | $\mid R_1 \wedge R_2$ | intersection |
| $\mid \rho, w \to y$ | assignment | $S ::=$ | **Inert type** |
| $c ::=$ | **Configuration** | $\mid \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T\}$ | object |
| $\mid \langle t; \sigma; \rho; \Sigma \rangle$ | | $\mathrm{F} ::=$ | **Inert context** |
| $\Gamma_{\mathrm{h}} ::=$ | **Heap Context** | $\mid$ | empty |
| $\mid \Gamma, y/s : R$ | | $\mid \mathrm{F}, y : S$ | binding |

### 3.12.1 Inert Context

In an inert context, all variables are locations ($y$) or references ($w$), all types are inert, which means they are of the form $\mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T\}$, where $R$ is a record type and $R$ **indep** $s$. A record type is an intersection of method, field and type member declarations with unique names. The type member declarations must be of the form $\{A(r) : T..T\}$ or $\{A(r) : \bot..T\}$. The field declarations must be of the form $\{a : T..T\}$. The type of variable $x$ can only refer to variables defined previously in the context (cannot refer to future variables or $x$ itself). General contexts are denoted by $\Gamma$, inert contexts by $\mathrm{F}$.

## 3.13 T-Free variables

A t-free variable $x$ in term $t$ is a free variable that occurs in $t$ not as a part of a type. That is, it occurs free as an operand in a subterm $\mathsf{v}x$, $x.a$, $x_1.a := x_2$ or $x_1.m\,x_2$, or in field definition $\{a = x\}$. Occurrences in

$x_1.B(x_2)$ do not count. Because locations cannot be bound in a let term or a method, all occurrences of $y$ other than $y.B(x)$ and $x.B(y)$ are t-free.

A t-free variable $x$ in stack $\sigma$, is a variable $x$ that is t-free in $t$, where $\mathsf{let}\ z = \Box\ \mathsf{in}\ t$ occurs in $\sigma$ and $x \neq z$.

Properties of t-free variables are stated in Section 5.2.1.

$$\frac{}{\mathsf{v}x\ \mathbf{tfree}\ x}\text{(TF-Var)}$$

$$\frac{}{x_1.m\,x_2\ \mathbf{tfree}\ x_1}\text{(TF-Apply1)}$$

$$\frac{}{x_1.m\,x_2\ \mathbf{tfree}\ x_2}\text{(TF-Apply2)}$$

$$\frac{}{x.a\ \mathbf{tfree}\ x}\text{(TF-Read)}$$

$$\frac{}{x_1.a := x_2\ \mathbf{tfree}\ x_1}\text{(TF-Write1)}$$

$$\frac{}{x_1.a := x_2\ \mathbf{tfree}\ x_2}\text{(TF-Write2)}$$

$$\frac{\begin{array}{c} d\ \mathbf{tfree}\ x \\ x \neq s \end{array}}{\mathsf{let}\ z = \nu(s : T_1)d\ \mathsf{in}\ t\ \mathbf{tfree}\ x}\text{(TF-NewD)}$$

$$\frac{\begin{array}{c} t\ \mathbf{tfree}\ x \\ x \neq z \end{array}}{\mathsf{let}\ z = \nu(s : T_1)d\ \mathsf{in}\ t\ \mathbf{tfree}\ x}\text{(TF-NewT)}$$

$$\frac{t_1\ \mathbf{tfree}\ x}{\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2\ \mathbf{tfree}\ x}\text{(TF-LetPush)}$$

$$\frac{\begin{array}{c} t_2\ \mathbf{tfree}\ x \\ x \neq z \end{array}}{\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2\ \mathbf{tfree}\ x}\text{(TF-LetPop)}$$

$$\frac{d_1\ \mathbf{tfree}\ x}{d_1 \wedge d_2\ \mathbf{tfree}\ x}\text{(TF-And1)}$$

$$\frac{d_2\ \mathbf{tfree}\ x}{d_1 \wedge d_2\ \mathbf{tfree}\ x}\text{(TF-And2)}$$

$$\frac{}{\{a = x\}\ \mathbf{tfree}\ x}\text{(TF-Fld)}$$

$$\frac{\begin{array}{c} t\ \mathbf{tfree}\ x \\ x \neq z \\ x \neq r \end{array}}{\{m(z, r) = t\}\ \mathbf{tfree}\ x}\text{(TF-Met)}$$

$$\frac{\begin{array}{c} t\ \mathbf{tfree}\ x \\ x \neq z \end{array}}{\mathsf{let}\ z = \Box\ \mathsf{in}\ t :: \sigma\ \mathbf{tfree}\ x}\text{(TF-LetST)}$$

$$\frac{\sigma\ \mathbf{tfree}\ x}{\mathsf{let}\ z = \Box\ \mathsf{in}\ t :: \sigma\ \mathbf{tfree}\ x}\text{(TF-LetSS)}$$

## 3.14 Mutable Objects

A location is *mutably reachable* from a configuration, if it is reachable from a mutable t-free variable $w$ in the term or on the stack through a sequence of fields, where every such field is not read-only

The set of mutably reachable locations changes in the following ways:

- On reduction of $\mathsf{let}\ z = \nu(s : T)d\ \mathsf{in}\ t$, the location of the new object is added.
- On reduction of $\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$, variables are moved between the term and stack, so mreach is not changed.
- On reduction of $w_1.a := w_2$, the old value of the field may be removed, if the field is mutable and there is no other mutable path to that object. If the field is readonly, then the new value may be removed.
- On reduction of $w.a$, the location corresponding to $w$ may be removed.
- On reduction of $w_1.m\,w_2$, the location corresponding to $w_1$ may be removed, and the location corresponding to $w_2$ may be removed if the parameter is not used in the body of the methods.

$$\frac{\begin{array}{c} \mathrm{F} \vdash \langle t; \sigma; \rho; \Sigma \rangle\ \mathbf{mreach}\ y_1 \\ y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma \\ \mathrm{F};\rho \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\} \end{array}}{\mathrm{F} \vdash \langle t; \sigma; \rho; \Sigma \rangle\ \mathbf{mreach}\ y_2}\text{(Rea-Fld)}$$

$$\frac{\begin{array}{c} t\ \mathbf{tfree}\ w \vee \sigma\ \mathbf{tfree}\ w \\ w \rightarrow y \in \rho \\ \mathrm{F};\rho \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\} \end{array}}{\mathrm{F} \vdash \langle t; \sigma; \rho; \Sigma \rangle\ \mathbf{mreach}\ y}\text{(Rea-Term)}$$

## 3.15 Reduction

The *reduction* relation defines each step of execution, transforming one machine configuration to the next. The term in the focus of execution decides which of the rules can be applied. For an answer, no rule applies, for other configurations, a single rule can be applied - this property is stated as the untyped progress lemma 5.174(Pg). For a given typed configuration, the next configuration is deterministic, up to fresh global variables added to the heap and context in the (R-LetNew) and (R-Read) rules.

$$\frac{\begin{array}{c} w_1 \rightarrow y_1 \in \rho_1 \\ y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma \\ \rho_2 = \rho_1, w_2 \rightarrow y_2 \end{array}}{\langle w_1.a; \sigma; \rho_1; \Sigma\rangle \longmapsto \langle \mathsf{v} w_2; \sigma; \rho_2; \Sigma\rangle}\text{(R-Read)}$$

$$\frac{\begin{array}{c} w_1 \rightarrow y_1 \in \rho \\ w_3 \rightarrow y_3 \in \rho \\ y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1 \\ \Sigma_2 = \Sigma_1[y_1 \rightarrow \ldots_1 \{a = y_3\} \ldots_2] \end{array}}{\langle w_1.a := w_3; \sigma; \rho; \Sigma_1\rangle \longmapsto \langle \mathsf{v} w_3; \sigma; \rho; \Sigma_2\rangle}\text{(R-Write)}$$

$$\frac{\begin{array}{c} w_1 \rightarrow y_1 \in \rho \\ y_1 \rightarrow \ldots_1 \{m(z, r) = t\} \ldots_2 \in \Sigma \end{array}}{\langle w_1.m\, w_2; \sigma; \rho; \Sigma\rangle \longmapsto \langle [w_1/r][w_2/z]t; \sigma; \rho; \Sigma\rangle}\text{(R-Apply)}$$

$$\frac{\begin{array}{c} \rho_2 = \rho_1, w \rightarrow y \\ \Sigma_2 = \Sigma_1, y \rightarrow [y/s][\rho_1]d \end{array}}{\langle \mathsf{let}\ z = \nu(s : T)d\ \mathsf{in}\ t; \sigma; \rho_1; \Sigma_1\rangle \longmapsto \langle [w/z]t; \sigma; \rho_2; \Sigma_2\rangle}\text{(R-LetNew)}$$

$$\frac{}{\langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma; \rho; \Sigma\rangle \longmapsto \langle t_1; \mathsf{let}\ z = \square\ \mathsf{in}\ t_2 :: \sigma; \rho; \Sigma\rangle}\text{(R-LetPush)}$$

$$\frac{}{\langle \mathsf{v} w; \mathsf{let}\ z = \square\ \mathsf{in}\ t :: \sigma; \rho; \Sigma\rangle \longmapsto \langle [w/z]t; \sigma; \rho; \Sigma\rangle}\text{(R-LetLoc)}$$

## 3.16 Configuration Typing

Correctly formed configurations have a type under an inert typing context F. The type is preserved during reduction, this property is stated in 5.171(TPP). The type of the configuration is the type of the lowest frame on the stack $\sigma$. The focus of execution $t$ must have the type expected by the highest frame on the stack. The environment $\rho$ must correspond to the typing context F. References must have the same type as the corresponding location, except their mutability may be different. The heap $\Sigma$ must also correspond to the typing context F. The definitions stored on the heap for location $y$ must have the type prescribed by F under heap typing rules.

$$\frac{\mathrm{F};\rho \vdash T_1 <: T_2}{\mathrm{F};\rho \vdash \cdot : T_1, T_2}\,(\text{CT-EmptyS})$$

$$\frac{\begin{array}{c} \mathrm{F};\rho \vdash \sigma : T_2, T_3 \\ \mathrm{F}, z : T_1;\rho \vdash t : T_2 \\ z \notin \text{fv } T_2 \end{array}}{\mathrm{F};\rho \vdash \mathsf{let}\ z = \Box\ \mathsf{in}\ t :: \sigma : T_1, T_3}\,(\text{CT-LetS})$$

$$\frac{}{\mathrm{F};\rho \vdash\sim .}\,(\text{CT-EmptyH})$$

$$\frac{}{\Gamma \sim .}\,(\text{CT-EmptyE})$$

$$\frac{\mathrm{F}_1;\rho \vdash \mathrm{F}_2 \sim \Sigma}{\mathrm{F}_1;\rho \vdash \mathrm{F}_2, w : T \sim \Sigma}\,(\text{CT-RefH})$$

$$\frac{\begin{array}{c} \mathrm{F}_1;\rho \vdash \mathrm{F}_2 \sim \Sigma \\ \mathrm{F}_1, y/s : R;\rho \vdash d : [y/s]R \\ R\ \textbf{indep}\ s \end{array}}{\mathrm{F}_1;\rho \vdash \mathrm{F}_2, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} \sim \Sigma, y \to d}\,(\text{CT-ObjH})$$

$$\frac{\begin{array}{c} \Gamma_1 \sim \rho \\ \Gamma = \Gamma_1, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T\}, \Gamma_2 \\ \Gamma_1 = \Gamma_3, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_4 \end{array}}{\Gamma \sim \rho, w \to y}\,(\text{CT-RefE})$$

$$\frac{\begin{array}{c} \mathrm{F};\rho \vdash \mathrm{F} \sim \Sigma \\ \text{all fields in } \Sigma \text{ are locations} \end{array}}{\mathrm{F};\rho \sim \Sigma}\,(\text{CT-CorrH})$$

$$\frac{\begin{array}{c} \mathrm{F} \sim \rho \\ \mathrm{F};\rho \sim \Sigma \\ \mathrm{F};\rho \vdash t : T_1 \\ \mathrm{F};\rho \vdash \sigma : T_1, T_2 \\ \text{no locations in } t \text{ and } \sigma \end{array}}{\mathrm{F} \vdash \langle t; \sigma; \rho; \Sigma \rangle : T_2}\,(\text{CT-Corr})$$

# 4 Internal Definitions

This section contains additional definitions which are used to state lemmata and prove the main theorems about roDOT.

## 4.1 Typed Reduction

For the purpose of proofs of the main theorems 5.173(S) and 5.181(IG), we define *typed reduction*, which a variant of the reduction relation which requires the configuration to be typed in a typing context F, and also defines how the typing context is extended.

$$\frac{\begin{array}{c} t_0 = w_1.a \\ \mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\ \mathrm{F};\rho_1 \vdash w_1 : \{a : T_4..T_3\} \\ \mathrm{F};\rho_1 \vdash T_3 \ \mathbf{mu}(r)\ T_7 \\ w_1 \rightarrow y_1 \in \rho_1 \\ \mathrm{F} = \mathrm{F}_3, y_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_4 \\ T_2 = \mu(s_1 : R_1) \wedge \{\mathsf{M}(r) : \bot..(T_7 \vee w_1.\mathsf{M}(r))\} \\ y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1 \\ \rho_2 = \rho_1, w_2 \rightarrow y_2 \end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v} w_2; \sigma_1; \rho_2; \Sigma_1 \rangle} (\text{TR}'\text{-Read})$$

$$\frac{\begin{array}{c} t_0 = w_1.a := w_3 \\ \mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\ w_1 \rightarrow y_1 \in \rho_1 \\ w_3 \rightarrow y_3 \in \rho_1 \\ y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1 \\ \Sigma_2 = \Sigma_1[y_1 \rightarrow \ldots_1 \{a = y_3\} \ldots_2] \end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle \mathsf{v} w_3; \sigma_1; \rho_1; \Sigma_2 \rangle} (\text{TR}'\text{-Write})$$

$$\frac{\begin{array}{c} t_0 = w_1.m\, w_2 \\ \mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\ w_1 \rightarrow y_1 \in \rho_1 \\ y_1 \rightarrow \ldots_1 \{m(z, r) = t\} \ldots_2 \in \Sigma_1 \end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/r][w_2/z]t; \sigma_1; \rho_1; \Sigma_1 \rangle} (\text{TR}'\text{-Apply})$$

$$\frac{\begin{array}{c} t_0 = \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t \\ \mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\ T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} \\ \Sigma_2 = \Sigma_1, y_1 \rightarrow [y_1/s][\rho_1]d \\ \rho_2 = \rho_1, w_1 \rightarrow y_1 \end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2 \rangle} (\text{TR}'\text{-LetNew})$$

$$\frac{\begin{array}{c} t_0 = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2 \\ \mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\ \sigma_2 = \mathsf{let}\ z = \square\ \mathsf{in}\ t_2 :: \sigma_1 \end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1 \rangle} (\text{TR}'\text{-LetPush})$$

$$\frac{\begin{array}{c} t_0 = \mathsf{v} w_1 \\ \mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\ \sigma_1 = \mathsf{let}\ z = \square\ \mathsf{in}\ t :: \sigma_2 \end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/z]t; \sigma_2; \rho_1; \Sigma_1 \rangle} (\text{TR}'\text{-LetLoc})$$

## 4.2 Typed Reduction Inlined

For convenience, we use a variant of typed reduction rules with premises of typing rules inlined into the reduction rule. Equivalence of typed reduction and normal reduction is stated in Section 5.3.8.

$$\dfrac{\begin{array}{c}
t_0 = w_1.a \\
\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\
\mathrm{F};\rho_1 \vdash w_1.a : T_1 \\
\mathrm{F};\rho_1 \vdash w_1 : \{a : T_4..T_3\} \\
\mathrm{F};\rho_1 \vdash T_3 \;\mathbf{ro}\; T_6 \\
\mathrm{F};\rho_1 \vdash T_3 \;\mathbf{mu}(r)\; T_7 \\
T_1 = T_6 \wedge \{\mathsf{M}(r) : \bot..(T_7 \vee w_1.\mathsf{M}(r))\} \\
w_1 \rightarrow y_1 \in \rho_1 \\
\mathrm{F};\rho_1 \vdash y_2 : [y_1/s]T_5 \\
T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} \\
R = \ldots_3 \{a : T_5..T_5\} \ldots_4 \\
\mathrm{F};\rho_1 \vdash T_4 <: [y_1/s]T_5 \\
\mathrm{F};\rho_1 \vdash [y_1/s]T_5 <: T_3 \\
\mathrm{F} = \mathrm{F}_1, y_1 : T, \mathrm{F}_2 \\
\mathrm{F} = \mathrm{F}_3, y_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_4 \\
T_2 = \mu(s_1 : R_1) \wedge \{\mathsf{M}(r) : \bot..(T_7 \vee w_1.\mathsf{M}(r))\} \\
y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1 \\
\rho_2 = \rho_1, w_2 \rightarrow y_2 \\
\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0
\end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1 \rangle} \text{(TR-Read)}$$

$$\dfrac{\begin{array}{c}
t_0 = w_1.a := w_3 \\
\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\
\mathrm{F};\rho_1 \vdash w_1.a := w_3 : T_1 \\
\mathrm{F};\rho_1 \vdash w_1 : \{a : T_3..T_2\} \\
w_1 \rightarrow y_1 \in \rho_1 \\
w_3 \rightarrow y_3 \in \rho_1 \\
\mathrm{F};\rho_1 \vdash w_1 : \{\mathsf{M}(r_0) : \bot..\bot\} \\
\mathrm{F};\rho_1 \vdash w_3 : T_3 \\
T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} \\
R = \ldots_3 \{a : T_4..T_4\} \ldots_4 \\
\mathrm{F};\rho_1 \vdash T_3 <: [y_1/s]T_4 \\
\mathrm{F};\rho_1 \vdash [y_1/s]T_4 <: T_2 \\
\mathrm{F} = \mathrm{F}_1, y_1 : T, \mathrm{F}_2 \\
y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1 \\
\Sigma_2 = \Sigma_1[y_1 \rightarrow \ldots_1 \{a = y_3\} \ldots_2] \\
\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0
\end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle \mathsf{v}w_3; \sigma_1; \rho_1; \Sigma_2 \rangle} \text{(TR-Write)}$$

$$\frac{\begin{array}{c}
t_0 = w_1.m\, w_2 \\
\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\
\mathrm{F};\rho_1 \vdash w_1.m\, w_2 : T_1 \\
\mathrm{F};\rho_1 \vdash w_1 : \{m(z : T_3, r : T_5) : T_4\} \\
T_1 = [w_1/r][w_2/z]T_4 \\
T_6 = [y_1/s]T_9 \\
T_8 = [y_1/s]T_{11} \\
T_7 = [y_1/s]T_{10} \\
w_1 \rightarrow y_1 \in \rho_1 \\
\mathrm{F};\rho_1 \vdash w_1 : [w_2/z]T_5 \\
\mathrm{F}, !, z : T_6, r : [y_1/s]R \wedge [r/s]R \wedge T_8;\rho_1 \vdash t : T_7 \\
\mathrm{F};\rho_1 \vdash w_2 : T_3 \\
T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} \\
R = \ldots_3 \{m(z : T_9, r : T_{11}) : T_{10}\} \ldots_4 \\
\mathrm{F};\rho_1 \vdash T_3 <: T_6 \\
\mathrm{F}, z : T_3;\rho_1 \vdash T_5 <: T_8 \\
\mathrm{F}, z : T_3, r : T_5;\rho_1 \vdash T_7 <: T_4 \\
\mathrm{F} = \mathrm{F}_1, y_1 : T, \mathrm{F}_2 \\
y_1 \rightarrow \ldots_1 \{m(z, r) = t\} \ldots_2 \in \Sigma_1 \\
\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0
\end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/r][w_2/z]t; \sigma_1; \rho_1; \Sigma_1 \rangle}\text{(TR-Apply)}$$

$$\frac{\begin{array}{c}
t_0 = \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t \\
\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\
\mathrm{F};\rho_1 \vdash \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t : T_1 \\
\mathrm{F}, z : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho_1 \vdash t : T_1 \\
\mathrm{F}, s : R;\rho_1 \vdash d : R \\
T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} \\
\Sigma_2 = \Sigma_1, y_1 \rightarrow [y_1/s][\rho_1]d \\
\rho_2 = \rho_1, w_1 \rightarrow y_1 \\
\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0
\end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2 \rangle}\text{(TR-LetNew)}$$

$$\frac{\begin{array}{c}
t_0 = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2 \\
\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\
\mathrm{F};\rho_1 \vdash \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2 : T_1 \\
\mathrm{F}, z : T_3;\rho_1 \vdash t_2 : T_1 \\
\mathrm{F};\rho_1 \vdash t_1 : T_3 \\
\sigma_2 = \mathsf{let}\ z = \square\ \mathsf{in}\ t_2 :: \sigma_1 \\
\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0
\end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1 \rangle}\text{(TR-LetPush)}$$

$$\frac{\begin{array}{c}
t_0 = \mathsf{v}w_1 \\
\mathrm{F} \vdash \langle \mathsf{v}w_1; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \\
\mathrm{F};\rho_1 \vdash \mathsf{v}w_1 : T_1 \\
\sigma_1 = \mathsf{let}\ z = \square\ \mathsf{in}\ t :: \sigma_2 \\
\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0
\end{array}}{\mathrm{F} \vdash \langle t_0; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/z]t; \sigma_2; \rho_1; \Sigma_1 \rangle}\text{(TR-LetLoc)}$$

## 4.3 Precise Typing

Precise typing is a limited variant of variable typing, defined in an inert context, similarly to kDOT [2]. It gives a reference or a location precise types of their members. Related properties are stated in Section 5.2.2.

$$\frac{\mathrm{F} = \mathrm{F}_1, v : T, \mathrm{F}_2}{\mathrm{F} \vdash_{!} v : T}\,(\text{VT}_{!}\text{-Var}) \qquad \frac{\mathrm{F} \vdash_{!} v : T_1 \wedge T_2}{\mathrm{F} \vdash_{!} v : T_1}\,(\text{VT}_{!}\text{-And1})$$

$$\frac{\mathrm{F} \vdash_{!} v : \mu(s : T)}{\mathrm{F} \vdash_{!} v : [v/s]T}\,(\text{VT}_{!}\text{-Rec}) \qquad \frac{\mathrm{F} \vdash_{!} v : T_1 \wedge T_2}{\mathrm{F} \vdash_{!} v : T_2}\,(\text{VT}_{!}\text{-And2})$$

## 4.4 Simplified Precise Typing

For convenience, we also use a variant of precise typing which uses the specific form of types that variables have in an inert context, and has fewer rules.

$$\frac{\begin{array}{c}\mathrm{F} = \mathrm{F}_1, v : \mu(s : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T\}, \mathrm{F}_2 \\ [v/s]R_1 = \dots_1 R_2 \dots_2\end{array}}{\mathrm{F} \vdash_{!1} v : R_2}\,(\text{VT}_{!1}\text{-Var})$$

$$\frac{\mathrm{F} = \mathrm{F}_1, v : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T\}, \mathrm{F}_2}{\mathrm{F} \vdash_{!2} v : \{\mathsf{M}(r_0) : \bot..T\}}\,(\text{VT}_{!2}\text{-Var})$$

## 4.5 Tight Typing

*Tight typing* is a limited variant of variable typing, defined in an inert context, similarly to kDOT [2]. Tight typing is only defined for (global) variables, not for terms. The only difference between tight and normal variable typing is the use of tight subtyping.

$$\frac{\mathrm{F} = \mathrm{F}_1, v : T, \mathrm{F}_2}{\mathrm{F};\rho \vdash_{\#} v : T}\,(\text{VT}_{\#}\text{-Var}) \qquad \frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} v : \mu(s : T) \\ T\ \textbf{indep}\ s\end{array}}{\mathrm{F};\rho \vdash_{\#} v : [v/s]T}\,(\text{VT}_{\#}\text{-RecE})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} v : T_1 \\ \mathrm{F};\rho \vdash_{\#} T_1 <: T_2\end{array}}{\mathrm{F};\rho \vdash_{\#} v : T_2}\,(\text{VT}_{\#}\text{-Sub}) \qquad \frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} v : [v/s]T \\ T\ \textbf{indep}\ s \\ \mathrm{F};\rho \vdash [v/s]T\ \textbf{ro}\ [v/s]T\end{array}}{\mathrm{F};\rho \vdash_{\#} v : \mu(s : T)}\,(\text{VT}_{\#}\text{-RecI})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} v : T_1 \\ \mathrm{F};\rho \vdash_{\#} v : T_2\end{array}}{\mathrm{F};\rho \vdash_{\#} v : T_1 \wedge T_2}\,(\text{VT}_{\#}\text{-AndI}) \qquad \frac{\mathrm{F};\rho \vdash_{\#} v : T}{\mathrm{F};\rho \vdash_{\#} v : \{\mathsf{M}(r_0) : \bot..\top\}}\,(\text{VT}_{\#}\text{-MutTop})$$

## 4.6 Tight Subtyping

*Tight subtyping* is a limited variant of subtyping, defined in an inert context, similarly to kDOT [2]. The difference between tight and normal subtyping is in the ($\text{ST}_{\#}$-SelL) and ($\text{ST}_{\#}$-SelU) rules, where normal typing uses normal typing of the variable, but tight subtyping uses precise typing to find the bound of the type member.

$$\frac{}{\mathrm{F};\rho \vdash_{\#} T <: T}(\mathrm{ST}_{\#}\text{-Refl})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} T_1 <: T_2\\ \mathrm{F};\rho \vdash_{\#} T_2 <: T_3\end{array}}{\mathrm{F};\rho \vdash_{\#} T_1 <: T_3}(\mathrm{ST}_{\#}\text{-Trans})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} T <: \top}(\mathrm{ST}_{\#}\text{-Top})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} \bot <: T}(\mathrm{ST}_{\#}\text{-Bot})$$

$$\frac{\rho \vdash T_1 \approx T_2}{\mathrm{F};\rho \vdash_{\#} T_1 <: T_2}(\mathrm{ST}_{\#}\text{-Eq})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} T_1 <: T_1 \vee T_2}(\mathrm{ST}_{\#}\text{-Or1})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} T_2 <: T_1 \vee T_2}(\mathrm{ST}_{\#}\text{-Or2})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} T_1 <: T_3\\ \mathrm{F};\rho \vdash_{\#} T_2 <: T_3\end{array}}{\mathrm{F};\rho \vdash_{\#} T_1 \vee T_2 <: T_3}(\mathrm{ST}_{\#}\text{-Or})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} T_1 <: T_2\\ \mathrm{F};\rho \vdash_{\#} T_1 <: T_3\end{array}}{\mathrm{F};\rho \vdash_{\#} T_1 <: T_2 \wedge T_3}(\mathrm{ST}_{\#}\text{-And})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} T_1 \wedge T_2 <: T_1}(\mathrm{ST}_{\#}\text{-And1})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} T_1 \wedge T_2 <: T_2}(\mathrm{ST}_{\#}\text{-And2})$$

$$\frac{\mathrm{F} \vdash_{!} v : \{B(r) : T_1..T_2\}}{\mathrm{F};\rho \vdash_{\#} [x_2/r]T_1 <: v.B(x_2)}(\mathrm{ST}_{\#}\text{-SelL})$$

$$\frac{\mathrm{F} \vdash_{!} v : \{B(r) : T_1..T_2\}}{\mathrm{F};\rho \vdash_{\#} v.B(x_2) <: [x_2/r]T_2}(\mathrm{ST}_{\#}\text{-SelU})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} T_3 <: T_1\\ \mathrm{F};\rho \vdash_{\#} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash_{\#} \{B(r) : T_1..T_2\} <: \{B(r) : T_3..T_4\}}(\mathrm{ST}_{\#}\text{-Typ})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} T_3 <: T_1\\ \mathrm{F};\rho \vdash_{\#} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash_{\#} \{a : T_1..T_2\} <: \{a : T_3..T_4\}}(\mathrm{ST}_{\#}\text{-Fld})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: \bot}(\mathrm{ST}_{\#}\text{-N-M})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} \mathsf{N} <: \mu(s : T)}(\mathrm{ST}_{\#}\text{-N-Rec})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} \mathsf{N} <: \{a : T_1..T_2\}}(\mathrm{ST}_{\#}\text{-N-Fld})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} \mathsf{N} <: \{A(r) : T_1..T_2\}}(\mathrm{ST}_{\#}\text{-N-Typ})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} T_3 <: T_1\\ \mathrm{F}, z : T_3;\rho \vdash T_6 <: T_5\\ \mathrm{F}, z : T_3, r : T_6;\rho \vdash T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash_{\#} \{m(z : T_1, r : T_5) : T_2\} <: \{m(z : T_3, r : T_6) : T_4\}}(\mathrm{ST}_{\#}\text{-Met})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} \mathsf{N} <: \{m(z : T_1, r : T_3) : T_2\}}(\mathrm{ST}_{\#}\text{-N-Met})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} \{B(r) : T_1..T_2\} \wedge \{B(r) : T_3..T_4\} <: \{B(r) : T_1 \vee T_3..T_2 \wedge T_4\}}(\mathrm{ST}_{\#}\text{-TypAnd})$$

$$\frac{}{\mathrm{F};\rho \vdash_{\#} T_1 \wedge (T_2 \vee T_3) <: (T_1 \wedge T_2) \vee (T_1 \wedge T_3)}(\mathrm{ST}_{\#}\text{-Dist})$$

## 4.7 Invertible Typing

*Invertible typing* is a limited variant of variable typing, defined in an inert context, similarly to kDOT [2]. Properties of invertible typing are stated in section 5.2.3. Equivalence of normal and invertible typing in an inert context is stated in Section 5.2.5.

$$\frac{\mathrm{F} \vdash_{!} v : T}{\mathrm{F};\rho \vdash_{\#\#} v : T}\text{(VT}_{\#\#}\text{-Var)}$$

$$\frac{\mathrm{F};\rho \vdash_{\#\#} v : T}{\mathrm{F};\rho \vdash_{\#\#} v : \top}\text{(VT}_{\#\#}\text{-Top)}$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#\#} v : T_1 \\ \mathrm{F};\rho \vdash_{\#\#} v : T_2\end{array}}{\mathrm{F};\rho \vdash_{\#\#} v : T_1 \wedge T_2}\text{(VT}_{\#\#}\text{-AndI)}$$

$$\frac{\mathrm{F};\rho \vdash_{\#\#} v : T_1}{\mathrm{F};\rho \vdash_{\#\#} v : T_1 \vee T_2}\text{(VT}_{\#\#}\text{-Or1)}$$

$$\frac{\mathrm{F};\rho \vdash_{\#\#} v : T_2}{\mathrm{F};\rho \vdash_{\#\#} v : T_1 \vee T_2}\text{(VT}_{\#\#}\text{-Or2)}$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#\#} v : [v/s]T \\ T\ \textbf{indep}\ s \\ \mathrm{F};\rho \vdash [v/s]T\ \textbf{ro}\ [v/s]T\end{array}}{\mathrm{F};\rho \vdash_{\#\#} v : \mu(s : T)}\text{(VT}_{\#\#}\text{-RecI)}$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#\#} v_1 : [v_3/r]T_1 \\ \mathrm{F} \vdash_{!} v_2 : \{B(r) : T_1..T_2\}\end{array}}{\mathrm{F};\rho \vdash_{\#\#} v_1 : v_2.B(v_3)}\text{(VT}_{\#\#}\text{-Sel)}$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#\#} v : \{B(r) : T_1..T_2\} \\ \mathrm{F};\rho \vdash_{\#} T_3 <: T_1 \\ \mathrm{F};\rho \vdash_{\#} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash_{\#\#} v : \{B(r) : T_3..T_4\}}\text{(VT}_{\#\#}\text{-Typ)}$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#\#} v : \{m(z : T_1, r : T_5) : T_2\} \\ \mathrm{F};\rho \vdash_{\#} T_3 <: T_1 \\ \mathrm{F}, z : T_3;\rho \vdash T_6 <: T_5 \\ \mathrm{F}, z : T_3, r : T_6;\rho \vdash T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash_{\#\#} v : \{m(z : T_3, r : T_6) : T_4\}}\text{(VT}_{\#\#}\text{-Met)}$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#\#} v : \{a : T_1..T_2\} \\ \mathrm{F};\rho \vdash_{\#} T_3 <: T_1 \\ \mathrm{F};\rho \vdash_{\#} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash_{\#\#} v : \{a : T_3..T_4\}}\text{(VT}_{\#\#}\text{-Fld)}$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#\#} v : T_1 \\ \rho \vdash T_1 \approx T_2\end{array}}{\mathrm{F};\rho \vdash_{\#\#} v : T_2}\text{(VT}_{\#\#}\text{-Eq)}$$

## 4.8 Selection Inlining Reduction

A *selection inlining reduction* is a relation between two types which allows replacing type selections by their bounds in one direction $\delta$. The direction $\oplus$ used in covariant positions replaces by upper bounds. The result type is a supertype of the original type. The direction $\ominus$ used in contravariant positions replaces by lower bounds. The result type is a subtype of the original type. Related properties are stated in Section 5.2.7.

$$\frac{}{\mathrm{F} \vdash T \longmapsto^{\mathrm{s}}_{\delta} T}(\mathrm{TR}^{\mathrm{s}}\text{-Refl})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_1..T_2\} \\ \mathrm{F} \vdash [x_2/r]T_2 \longmapsto^{\mathrm{s}}_{\oplus} T_3\end{array}}{\mathrm{F} \vdash v_1.B(x_2) \longmapsto^{\mathrm{s}}_{\oplus} T_3}(\mathrm{TR}^{\mathrm{s}}\text{-SelU})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_1..T_2\} \\ \mathrm{F} \vdash [x_2/r]T_1 \longmapsto^{\mathrm{s}}_{\ominus} T_3\end{array}}{\mathrm{F} \vdash v_1.B(x_2) \longmapsto^{\mathrm{s}}_{\ominus} T_3}(\mathrm{TR}^{\mathrm{s}}\text{-SelL})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3 \\ \mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4\end{array}}{\mathrm{F} \vdash T_1 \wedge T_2 \longmapsto^{\mathrm{s}}_{\delta} T_3 \wedge T_4}(\mathrm{TR}^{\mathrm{s}}\text{-And})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3 \\ \mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4\end{array}}{\mathrm{F} \vdash T_1 \vee T_2 \longmapsto^{\mathrm{s}}_{\delta} T_3 \vee T_4}(\mathrm{TR}^{\mathrm{s}}\text{-Or})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{-\delta} T_3 \\ \mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4\end{array}}{\mathrm{F} \vdash \{a : T_1..T_2\} \longmapsto^{\mathrm{s}}_{\delta} \{a : T_3..T_4\}}(\mathrm{TR}^{\mathrm{s}}\text{-Fld})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{-\delta} T_3 \\ \mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4\end{array}}{\mathrm{F} \vdash \{B(r) : T_1..T_2\} \longmapsto^{\mathrm{s}}_{\delta} \{B(r) : T_3..T_4\}}(\mathrm{TR}^{\mathrm{s}}\text{-Typ})$$

## 4.9 Method Type Approximation Reduction

A *method type approximation reduction* is a relation between two types which replaces method types by $\top$ or $\bot$. The direction $\oplus$ used in covariant positions replaces by $\top$. The result type is a supertype of the original type. The direction $\ominus$ used in contravariant positions replaces by $\bot$. The result type is a subtype of the original type. Related properties are stated in Section 5.2.7.

$$\frac{}{\top \longmapsto^{\mathrm{m}}_{\delta} \top}(\mathrm{TR}^{\mathrm{m}}\text{-Top})$$

$$\frac{}{\bot \longmapsto^{\mathrm{m}}_{\delta} \bot}(\mathrm{TR}^{\mathrm{m}}\text{-Bot})$$

$$\frac{}{\mathsf{N} \longmapsto^{\mathrm{m}}_{\oplus} \mathsf{N}}(\mathrm{TR}^{\mathrm{m}}\text{-N})$$

$$\frac{}{\mathsf{N} \longmapsto^{\mathrm{m}}_{\ominus} \bot}(\mathrm{TR}^{\mathrm{m}}\text{-N-Bot})$$

$$\frac{}{v_1.B(x_2) \longmapsto^{\mathrm{m}}_{\delta} v_1.B(x_2)}(\mathrm{TR}^{\mathrm{m}}\text{-Sel})$$

$$\frac{}{\mu(s : T_1) \longmapsto^{\mathrm{m}}_{\delta} \mu(s : T_1)}(\mathrm{TR}^{\mathrm{m}}\text{-Rec})$$

$$\frac{\begin{array}{c}T_1 \longmapsto^{\mathrm{m}}_{\delta} T_3\\ T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4\end{array}}{T_1 \wedge T_2 \longmapsto^{\mathrm{m}}_{\delta} T_3 \wedge T_4}(\mathrm{TR}^{\mathrm{m}}\text{-And})$$

$$\frac{\begin{array}{c}T_1 \longmapsto^{\mathrm{m}}_{\delta} T_3\\ T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4\end{array}}{T_1 \vee T_2 \longmapsto^{\mathrm{m}}_{\delta} T_3 \vee T_4}(\mathrm{TR}^{\mathrm{m}}\text{-Or})$$

$$\frac{\begin{array}{c}T_1 \longmapsto^{\mathrm{m}}_{-\delta} T_3\\ T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4\end{array}}{\{a : T_1..T_2\} \longmapsto^{\mathrm{m}}_{\delta} \{a : T_3..T_4\}}(\mathrm{TR}^{\mathrm{m}}\text{-Fld})$$

$$\frac{\begin{array}{c}T_1 \longmapsto^{\mathrm{m}}_{-\delta} T_3\\ T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4\end{array}}{\{B(r) : T_1..T_2\} \longmapsto^{\mathrm{m}}_{\delta} \{B(r) : T_3..T_4\}}(\mathrm{TR}^{\mathrm{m}}\text{-Typ})$$

$$\frac{}{\{m(z : T_1, r : T_3) : T_2\} \longmapsto^{\mathrm{m}}_{\oplus} \top}(\mathrm{TR}^{\mathrm{m}}\text{-MetU})$$

$$\frac{}{\{m(z : T_1, r : T_3) : T_2\} \longmapsto^{\mathrm{m}}_{\ominus} \bot}(\mathrm{TR}^{\mathrm{m}}\text{-MetL})$$

## 4.10 Selection Approximation Reduction

A *method type approximation reduction* is a relation between two types which allows replacing type selections types by $\top$ or $\bot$. The direction $\oplus$ used in covariant positions replaces by $\bot$. The direction $\ominus$ used in contravariant positions replaces by $\top$. Related properties are stated in Section 5.2.7 and Section 5.2.8.

$$\frac{}{v_1.B(x_2) \longmapsto^{\mathrm{e}}_{\oplus} \bot}(\text{TER-SelU})$$

$$\frac{}{v_1.B(x_2) \longmapsto^{\mathrm{e}}_{\ominus} \top}(\text{TER-SelL})$$

$$\frac{}{\top \longmapsto^{\mathrm{e}}_{\delta} \top}(\text{TER-Top})$$

$$\frac{}{v_1.B(x_2) \longmapsto^{\mathrm{e}}_{\delta} v_1.B(x_2)}(\text{TER-Sel})$$

$$\frac{}{\bot \longmapsto^{\mathrm{e}}_{\delta} \bot}(\text{TER-Bot})$$

$$\frac{}{\mu(s : T_1) \longmapsto^{\mathrm{e}}_{\delta} \mu(s : T_1)}(\text{TER-Rec})$$

$$\frac{}{\mathsf{N} \longmapsto^{\mathrm{e}}_{\oplus} \mathsf{N}}(\text{TER-N})$$

$$\frac{}{\mathsf{N} \longmapsto^{\mathrm{e}}_{\ominus} \bot}(\text{TER-N-Bot})$$

$$\frac{\begin{array}{c} T_1 \longmapsto^{\mathrm{e}}_{\delta} T_3 \\ T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4 \end{array}}{T_1 \wedge T_2 \longmapsto^{\mathrm{e}}_{\delta} T_3 \wedge T_4}(\text{TER-And})$$

$$\frac{\begin{array}{c} T_1 \longmapsto^{\mathrm{e}}_{\delta} T_3 \\ T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4 \end{array}}{T_1 \vee T_2 \longmapsto^{\mathrm{e}}_{\delta} T_3 \vee T_4}(\text{TER-Or})$$

$$\frac{\begin{array}{c} T_1 \longmapsto^{\mathrm{e}}_{-\delta} T_3 \\ T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4 \end{array}}{\{a : T_1..T_2\} \longmapsto^{\mathrm{e}}_{\delta} \{a : T_3..T_4\}}(\text{TER-Fld})$$

$$\frac{\begin{array}{c} T_1 \longmapsto^{\mathrm{e}}_{-\delta} T_3 \\ T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4 \end{array}}{\{B(r) : T_1..T_2\} \longmapsto^{\mathrm{e}}_{\delta} \{B(r) : T_3..T_4\}}(\text{TER-Typ})$$

$$\frac{}{\{m(z : T_1, r : T_3) : T_2\} \longmapsto^{\mathrm{e}}_{\oplus} \top}(\text{TER-MetU})$$

$$\frac{}{\{m(z : T_1, r : T_3) : T_2\} \longmapsto^{\mathrm{e}}_{\ominus} \bot}(\text{TER-MetL})$$

## 4.11 One Way Tight Subtyping

*One-way tight subtyping* is a limited variant of tight subtyping, which allows using the selection rules only in one direction $\delta$.

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} T <: \top}(\mathrm{ST}^{s}_{\#}\text{-Top})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} \bot <: T}(\mathrm{ST}^{s}_{\#}\text{-Bot})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} T <: T}(\mathrm{ST}^{s}_{\#}\text{-Refl})$$

$$\frac{\rho \vdash T_1 \approx T_2}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_2}(\mathrm{ST}^{s}_{\#}\text{-Eq})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_2 \\ \mathrm{F};\rho \vdash^{s}_{\delta} T_2 <: T_3\end{array}}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_3}(\mathrm{ST}^{s}_{\#}\text{-Trans})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_1 \vee T_2}(\mathrm{ST}^{s}_{\#}\text{-Or1})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} T_2 <: T_1 \vee T_2}(\mathrm{ST}^{s}_{\#}\text{-Or2})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_3 \\ \mathrm{F};\rho \vdash^{s}_{\delta} T_2 <: T_3\end{array}}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 \vee T_2 <: T_3}(\mathrm{ST}^{s}_{\#}\text{-Or})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} \mathsf{N} <: \mu(s : T)}(\mathrm{ST}^{s}_{\#}\text{-N-Rec})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} \mathsf{N} <: \{a : T_1..T_2\}}(\mathrm{ST}^{s}_{\#}\text{-N-Fld})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 \wedge T_2 <: T_1}(\mathrm{ST}^{s}_{\#}\text{-And1})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 \wedge T_2 <: T_2}(\mathrm{ST}^{s}_{\#}\text{-And2})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_2 \\ \mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_3\end{array}}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 <: T_2 \wedge T_3}(\mathrm{ST}^{s}_{\#}\text{-And})$$

$$\frac{\mathrm{F} \vdash_{!} v : \{B(r) : T_1..T_2\}}{\mathrm{F};\rho \vdash^{s}_{\oplus} v.B(x_2) <: [x_2/r]T_2}(\mathrm{ST}^{s}_{\#}\text{-SelU})$$

$$\frac{\mathrm{F} \vdash_{!} v : \{B(r) : T_1..T_2\}}{\mathrm{F};\rho \vdash^{s}_{\ominus} [x_2/r]T_1 <: v.B(x_2)}(\mathrm{ST}^{s}_{\#}\text{-SelL})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{s}_{-\delta} T_3 <: T_1 \\ \mathrm{F};\rho \vdash^{s}_{\delta} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash^{s}_{\delta} \{B(r) : T_1..T_2\} <: \{B(r) : T_3..T_4\}}(\mathrm{ST}^{s}_{\#}\text{-Typ})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{s}_{-\delta} T_3 <: T_1 \\ \mathrm{F};\rho \vdash^{s}_{\delta} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash^{s}_{\delta} \{a : T_1..T_2\} <: \{a : T_3..T_4\}}(\mathrm{ST}^{s}_{\#}\text{-Fld})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: \bot}(\mathrm{ST}^{s}_{\#}\text{-N-M})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} \mathsf{N} <: \{B(r) : T_1..T_2\}}(\mathrm{ST}^{s}_{\#}\text{-N-Typ})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash_{\#} T_3 <: T_1 \\ \mathrm{F}, z : T_3;\rho \vdash T_6 <: T_5 \\ \mathrm{F}, z : T_3, r : T_6;\rho \vdash T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash^{s}_{\delta} \{m(z : T_1, r : T_5) : T_2\} <: \{m(z : T_3, r : T_6) : T_4\}}(\mathrm{ST}^{s}_{\#}\text{-Met})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} \{B(r) : T_1..T_2\} \wedge \{B(r) : T_3..T_4\} <: \{B(r) : T_1 \vee T_3..T_2 \wedge T_4\}}(\mathrm{ST}^{s}_{\#}\text{-TypAnd})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} T_1 \wedge T_2 \vee T_3 <: (T_1 \wedge T_2) \vee (T_1 \wedge T_3)}(\mathrm{ST}^{s}_{\#}\text{-Dist})$$

$$\frac{}{\mathrm{F};\rho \vdash^{s}_{\delta} \mathsf{N} <: \{m(z : T_1, r : T_3) : T_2\}}(\mathrm{ST}^{s}_{\#}\text{-N-Met})$$

## 4.12 No Method Subtyping

*No-method tight subtyping* is a limited variant of tight subtyping, which allows using the selection rules only in one direction $\delta$, and does not have subtyping betwen method types.

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T <: \top}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Top})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \bot <: T}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Bot})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T <: T}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Refl})$$

$$\frac{\rho \vdash T_1 \approx T_2}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_2}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Eq})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_2\\ \mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_3\end{array}}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_3}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Trans})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_1 \vee T_2}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Or1})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_1 \vee T_2}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Or2})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_3\\ \mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_3\end{array}}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \vee T_2 <: T_3}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Or})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \mathsf{N} <: \mu(s : T)}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-N-Rec})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \mathsf{N} <: \{a : T_1..T_2\}}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-N-Fld})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_1}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-And1})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_2}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-And2})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_2\\ \mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_3\end{array}}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_2 \wedge T_3}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-And})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash_{!} v : \{B(r) : T_1..T_2\}\\ [x_2/r]T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_3\end{array}}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} v.B(x_2) <: T_3}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-SelU})$$

$$\frac{\begin{array}{c}\mathrm{F} \vdash_{!} v : \{B(r) : T_1..T_2\}\\ [x_2/r]T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_3\end{array}}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_3 <: v.B(x_2)}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-SelL})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{\mathrm{m}}_{-\delta} T_3 <: T_1\\ \mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \{B(r) : T_1..T_2\} <: \{B(r) : T_3..T_4\}}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Typ})$$

$$\frac{\begin{array}{c}\mathrm{F};\rho \vdash^{\mathrm{m}}_{-\delta} T_3 <: T_1\\ \mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_4\end{array}}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \{a : T_1..T_2\} <: \{a : T_3..T_4\}}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Fld})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: \bot}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-N-M})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \mathsf{N} <: \{A(r) : T_1..T_2\}}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-N-Typ})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} \{B(r) : T_1..T_2\} \wedge \{B(r) : T_3..T_4\} <: \{B(r) : T_1 \vee T_3..T_2 \wedge T_4\}}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-TypAnd})$$

$$\frac{}{\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 \vee T_3 <: (T_1 \wedge T_2) \vee (T_1 \wedge T_3)}(\mathrm{ST}^{\mathrm{m}}_{\#}\text{-Dist})$$

## 4.13 Type Without Selections

The relation $T$ **nosel** $x$ means that the type $T$ does not contain type selections involving $x$.

$$\frac{}{\top \ \mathbf{nosel}\ x}\text{(TN-Top)}$$

$$\frac{}{\bot \ \mathbf{nosel}\ x}\text{(TN-Bot)}$$

$$\frac{}{\mathsf{N} \ \mathbf{nosel}\ x}\text{(TN-N)}$$

$$\frac{\begin{array}{c} T_1 \ \mathbf{nosel}\ x \\ T_2 \ \mathbf{nosel}\ x \end{array}}{T_1 \wedge T_2 \ \mathbf{nosel}\ x}\text{(TN-And)}$$

$$\frac{\begin{array}{c} T_1 \ \mathbf{nosel}\ x \\ T_2 \ \mathbf{nosel}\ x \end{array}}{T_1 \vee T_2 \ \mathbf{nosel}\ x}\text{(TN-Or)}$$

$$\frac{\begin{array}{c} x_3 \neq x \\ x_3 \neq x_2 \end{array}}{x_1.B(x_2) \ \mathbf{nosel}\ x_3}\text{(TN-Sel)}$$

$$\frac{}{\mu(s : T) \ \mathbf{nosel}\ x}\text{(TN-Rec)}$$

$$\frac{\begin{array}{c} T_1 \ \mathbf{nosel}\ x \\ T_2 \ \mathbf{nosel}\ x \end{array}}{\{A(r) : T_1..T_2\} \ \mathbf{nosel}\ x}\text{(TN-Typ)}$$

$$\frac{\begin{array}{c} T_1 \ \mathbf{nosel}\ x \\ T_2 \ \mathbf{nosel}\ x \end{array}}{\{a : T_1..T_2\} \ \mathbf{nosel}\ x}\text{(TN-Fld)}$$

$$\frac{\begin{array}{c} T_1 \ \mathbf{nosel}\ x \\ T_2 \ \mathbf{nosel}\ x \\ T_3 \ \mathbf{nosel}\ x \end{array}}{\{m(z : T_1, r : T_3) : T_2\} \ \mathbf{nosel}\ x}\text{(TN-Met)}$$

# 5 Properties

This section contains lemmata and theorems with proofs.

## 5.1 Typing lemmata

This section states properties of typing relations in general contexts.

### 5.1.1 Equivalence lemmata

This section states properties of type equivalence (defined in Section 3.11). Two variables $v_1$ and $v_2$ are equivalent under $\rho$ if $v_1 \to v_2 \in \rho$, and this relation is reflexive, transitive and symmetric. Two types $T_1$ and $T_2$ are equivalent if they are syntactically the same up to equivalence of variables occurring on the left hand side of selection of normal type members.

First, we observe that variable equivalence is only defined for global variables, not for abstract variables.

**Lemma 5.1** (EqVKind)**.** *If $\rho \vdash x_1 \approx x_2$, then there exist $v_1$, $v_2$, such that $x_1 = v_1$, and $x_2 = v_2$.*

*Idea.* Variable equivalence only applies to locations and references. ▽

*Proof.* By inversion of $\rho \vdash x_1 \approx x_2$. □

Equivalence of types is also reflexive, transitive and symmetric. Reflexivity is ensured by (TE-Refl), but transitivity and symmetry has to be proven by induction, using the reflexivity and transitivity of variable equivalence.

**Lemma 5.2** (EqSymm)**.** *If $\rho \vdash T_1 \approx T_2$, then $\rho \vdash T_2 \approx T_1$.*

*Idea.* Type equivalence is symmetric. ▽

*Proof idea.* Straightforward induction on type and variable equivalence, with leaf cases swapped. ▽

*Proof.* Induction on $\rho \vdash T_1 \approx T_2$:

- Case (TE-Refl): $T_1 = T_2$. By (TE-Refl).
- Case (TE-Sel): $T_1 = x_1.A(x)$, and $T_2 = x_2.A(x)$, and $\rho \vdash x_1 \approx x_2$. By 5.1(EqVKind), exist $v_1$, $v_2$, such that $x_1 = v_1$, and $x_2 = v_2$. By (VE-Symm), $\rho \vdash x_2 \approx x_1$. By (TE-Sel).
- Case (TE-And): $T_1 = T_3 \wedge T_4$, and $T_2 = T_5 \wedge T_6$, where $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$. By induction, $\rho \vdash T_5 \approx T_3$, and $\rho \vdash T_6 \approx T_4$. By (TE-And).
- Case (TE-Or): $T_1 = T_3 \vee T_4$, and $T_2 = T_5 \vee T_6$, where $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$. By induction, $\rho \vdash T_5 \approx T_3$, and $\rho \vdash T_6 \approx T_4$. By (TE-Or).
- Case (TE-Rec): $T_1 = \mu(s : T_3)$, and $T_2 = \mu(s : T_4)$, where $\rho \vdash T_3 \approx T_4$. By induction, $\rho \vdash T_4 \approx T_3$. By (TE-Rec).
- Case (TE-Typ): $T_1 = \{B(r) : T_3..T_4\}$, and $T_2 = \{B(r) : T_5..T_6\}$, where $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$. By induction, $\rho \vdash T_5 \approx T_3$, and $\rho \vdash T_6 \approx T_4$. By (TE-Typ).
- Case (TE-Fld): $T_1 = \{a : T_3..T_4\}$, and $T_2 = \{a : T_5..T_6\}$, where $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$. By induction, $\rho \vdash T_5 \approx T_3$, and $\rho \vdash T_6 \approx T_4$. By (TE-Fld).
- Case (TE-Met): $T_1 = \{m(z : T_3, r : T_5) : T_4\}$, and $T_2 = \{m(z : T_6, r : T_8) : T_7\}$, where $\rho \vdash T_3 \approx T_6$, and $\rho \vdash T_4 \approx T_7$, and $\rho \vdash T_5 \approx T_8$. By induction, $\rho \vdash T_6 \approx T_3$, and $\rho \vdash T_7 \approx T_4$, and $\rho \vdash T_8 \approx T_5$. By (TE-Met).

□

**Lemma 5.3** (EqTrans)**.** *If $\rho \vdash T_1 \approx T_2$, and $\rho \vdash T_2 \approx T_3$, then $\rho \vdash T_1 \approx T_3$.*

*Idea.* Type equivalence is transitive. ▽

*Proof idea.* Straightforward induction on type and variable equivalence. ▽

*Proof.* If $T_2 = T_3$, then trivially. Induction on $\rho \vdash T_1 \approx T_2$:

- Case (TE-Refl): $T_1 = T_2$. Trivially.
- Case (TE-Sel): $T_1 = x_1.A(x)$, and $T_2 = x_2.A(x)$, and $\rho \vdash x_1 \approx x_2$. By inversion of (TE-Sel), $T_3 = x_3.A(x)$, and $\rho \vdash x_2 \approx x_3$. By 5.1(EqVKind), exist $v_1$, $v_2$, $v_3$, such that $x_1 = v_1$, and $x_2 = v_2$, and $x_3 = v_3$. By (VE-Trans), $\rho \vdash x_1 \approx x_3$. By (TE-Sel).
- Case (TE-And): $T_1 = T_4 \wedge T_5$, and $T_2 = T_6 \wedge T_7$, where $\rho \vdash T_4 \approx T_6$, and $\rho \vdash T_5 \approx T_7$. By inversion of (TE-And), $T_3 = T_8 \wedge T_9$, where $\rho \vdash T_6 \approx T_8$, and $\rho \vdash T_7 \approx T_9$. By induction, $\rho \vdash T_4 \approx T_8$, and $\rho \vdash T_5 \approx T_9$. By (TE-And).
- Case (TE-Or): $T_1 = T_4 \vee T_5$, and $T_2 = T_6 \vee T_7$, where $\rho \vdash T_4 \approx T_6$, and $\rho \vdash T_5 \approx T_7$. By inversion of (TE-Or), $T_3 = T_8 \vee T_9$, where $\rho \vdash T_6 \approx T_8$, and $\rho \vdash T_7 \approx T_9$. By induction, $\rho \vdash T_4 \approx T_8$, and $\rho \vdash T_5 \approx T_9$. By (TE-Or).
- Case (TE-Rec): $T_1 = \mu(s : T_4)$, and $T_2 = \mu(s : T_5)$, where $\rho \vdash T_4 \approx T_5$. By inversion of (TE-Rec), $T_3 = \mu(s : T_6)$, where $\rho \vdash T_5 \approx T_6$. By induction, $\rho \vdash T_4 \approx T_6$. By (TE-Rec).
- Case (TE-Typ): $T_1 = \{B(r) : T_4..T_5\}$, and $T_2 = \{B(r) : T_6..T_7\}$, where $\rho \vdash T_4 \approx T_6$, and $\rho \vdash T_5 \approx T_7$. By inversion of (TE-Typ), $T_3 = \{B(r) : T_8..T_9\}$, where $\rho \vdash T_6 \approx T_8$, and $\rho \vdash T_7 \approx T_9$. By induction, $\rho \vdash T_4 \approx T_8$, and $\rho \vdash T_5 \approx T_9$. By (TE-Typ).
- Case (TE-Fld): $T_1 = \{a : T_4..T_5\}$, and $T_2 = \{a : T_6..T_7\}$, where $\rho \vdash T_4 \approx T_6$, and $\rho \vdash T_5 \approx T_7$. By inversion of (TE-Fld), $T_3 = \{a : T_8..T_9\}$, where $\rho \vdash T_6 \approx T_8$, and $\rho \vdash T_7 \approx T_9$. By induction, $\rho \vdash T_4 \approx T_8$, and $\rho \vdash T_5 \approx T_9$. By (TE-Fld).
- Case (TE-Met): $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_2 = \{m(z : T_7, r : T_9) : T_8\}$, where $\rho \vdash T_4 \approx T_7$, and $\rho \vdash T_5 \approx T_8$, and $\rho \vdash T_6 \approx T_9$. By inversion of (TE-Met), $T_3 = \{m(z : T_{10}, r : T_{12}) : T_{11}\}$, where $\rho \vdash T_7 \approx T_{10}$, and $\rho \vdash T_8 \approx T_{11}$, and $\rho \vdash T_9 \approx T_{12}$. By induction, $\rho \vdash T_4 \approx T_{10}$, and $\rho \vdash T_5 \approx T_{11}$, and $\rho \vdash T_6 \approx T_{12}$. By (TE-Met).

□

Finally we state a lemma to be used in proofs by induction, where we invert equivalence of types, where one type has a known structure. Because of the (TE-Refl) rule, we cannot immediately say which one rule was used to derive the equivalence – whether (TE-Refl) or the rule specific to the structure of the type. This lemma states that in both cases the strucutre of the other type is necessarily the same.

**Lemma 5.4** (TEInv). *If $\rho \vdash T_1 \wedge T_2 \approx T_3$, then there exist $T_4$, $T_5$, such that $T_3 = T_4 \wedge T_5$, and $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$. If $\rho \vdash T_1 \vee T_2 \approx T_3$, then there exist $T_4$, $T_5$, such that $T_3 = T_4 \vee T_5$, and $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$. If $\rho \vdash \{a : T_1..T_2\} \approx T_3$, then there exist $T_4$, $T_5$, such that $T_3 = \{a : T_4..T_5\}$, and $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$. If $\rho \vdash \{B(r) : T_1..T_2\} \approx T_3$, then there exist $T_4$, $T_5$, such that $T_3 = \{B(r) : T_4..T_5\}$, and $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$. If $\rho \vdash \mu(s : T_1) \approx T_3$, then there exists $T_4$, such that $T_3 = \mu(s : T_4)$, and $\rho \vdash T_1 \approx T_4$.*

*Idea.* Type equivalence preserves the structure of a type. ▽

*Proof idea.* Inversion of type equivalence. In all cases, either a rule specific for the syntax can be used, or (TE-Refl). The specific rule premises directly correspond to the conclusions of the lemma. In case of the (TE-Refl) rule, we simply apply (TE-Refl) on the parts of the type. ▽

*Proof.*

- $T_1 \wedge T_2$: By inversion: Subcase (TE-Refl): $T_3 = T_1 \wedge T_2$. Choose $T_4 = T_1$, and $T_5 = T_2$. By (TE-Refl). Subcase (TE-And): $T_3 = T_4 \wedge T_5$, where $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$.
- $T_1 \vee T_2$: By inversion: Subcase (TE-Refl): $T_3 = T_1 \vee T_2$. Choose $T_4 = T_1$, and $T_5 = T_2$. By (TE-Refl). Subcase (TE-Or): $T_3 = T_4 \vee T_5$, where $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$.
- $\{a : T_1..T_2\}$: By inversion: Subcase (TE-Refl): $T_3 = \{a : T_1..T_2\}$. Choose $T_4 = T_1$, and $T_5 = T_2$. By (TE-Refl). Subcase (TE-Fld): $T_3 = \{a : T_4..T_5\}$, where $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$.
- $\{B(r) : T_1..T_2\}$: By inversion: Subcase (TE-Refl): $T_3 = \{B(r) : T_1..T_2\}$. Choose $T_4 = T_1$, and $T_5 = T_2$. By (TE-Refl). Subcase (TE-Typ): $T_3 = \{B(r) : T_4..T_5\}$, where $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$.
- $\mu(s : T_1)$: By inversion: Subcase (TE-Refl): $T_3 = \mu(s : T_1)$. Choose $T_4 = T_1$. By (TE-Refl). Subcase (TE-Rec): $T_3 = \mu(s : T_4)$, where $\rho \vdash T_1 \approx T_4$.

□

### 5.1.2 Typing context lemmata

This section contains lemmata about typing and subtyping in different contexts, notably the weakening 5.5(Wkn) and narrowing 5.13(Narr) lemmata. Their proofs are same or similar to their counterparts in kDOT [2].

First, the weakening lemmata 5.5(Wkn), 5.6(WknS) and 5.7(WknE) state that various kinds of typing, subtyping, visibility, splitting and environment correspondence is preserved if the typing context is extended with more variables.

**Lemma 5.5** (Wkn). *The following holds for typing, subtyping and splitting:*

- *If* $\Gamma_1, \Gamma_2$ **vis** $x$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x$.
- *If* $\Gamma_1, \Gamma_2;\rho \vdash x : T_1$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : T_1$.
- *If* $\Gamma_1, \Gamma_2;\rho \vdash T_3 <: T_1$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3 <: T_1$.
- *If* $\Gamma_1, \Gamma_2;\rho \vdash T_3\ \mathbf{ro}\ T_1$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3\ \mathbf{ro}\ T_1$.
- *If* $\Gamma_1, \Gamma_2;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$.
- *If* $\Gamma_1, \Gamma_2;\rho \vdash t : T_1$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : T_1$.
- *If* $\Gamma_1, \Gamma_2, s : T_3;\rho \vdash d : T_1$*, and* $x_2 \neq s$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3;\rho \vdash d : T_1$.
- *If* $\Gamma_1, \Gamma_2, y/s : T_3;\rho \vdash d : T_1$*, and* $x_2 \neq s$*, and* $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$*, then* $\Gamma_1, x_2 : T_2, \Gamma_2, y/s : T_3;\rho \vdash d : T_1$.

*Idea.* Adding variables to a context preserves typing. ▽

*Proof idea.* Induction on variable typing, term typing, definition typing, subtyping and splitting ▽

*Proof.* Mutual induction:

- Case (Vis-Var): $\Gamma_1, \Gamma_2 = \Gamma_3, x : T_4, \Gamma_4$, and $! \notin \Gamma_4$. The variable $x_2$ will be inserted into $\Gamma_3$ or $\Gamma_4$, so there is $\Gamma_1, x_2 : T_2, \Gamma_2 = \Gamma_5, x : T_4, \Gamma_6$, and $! \notin \Gamma_6$. By (Vis-Var), $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x$.
- Case (VT-Var): $\Gamma_1, \Gamma_2 = \Gamma_3, x : T_1, \Gamma_4$. Because $x_2 \notin \mathrm{dom}\ \Gamma_1, \Gamma_2$, then $x_2 \neq x$. Then $x_2 : T_2$ is added into $\Gamma_3$ or $\Gamma_4$ and (VT-Var) applies the same.
- Case (VT-RecE): $T_1 = [x/s]T_4$, and $\Gamma_1, \Gamma_2;\rho \vdash x : \mu(s : T_4)$, and $T_4$ **indep** $s$.

  By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : \mu(s : T_4)$. By (VT-RecE), $\Gamma_1, x_2 : T_2, \Gamma_2; \rho \vdash x : [x/s]T_4$.
- Case (VT-RecI): $\Gamma_1, \Gamma_2;\rho \vdash x : [x/s]T_4$, and $T_1 = \mu(s : T_4)$, and $\Gamma_1, \Gamma_2;\rho \vdash [x/s]T_4\ \mathbf{ro}\ [x/s]T_4$, and $T_4$ **indep** $s$.

  By induction on ro splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash [x/s]T_4\ \mathbf{ro}\ [x/s]T_4$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : [x/s]T_4$. By (VT-RecI), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : \mu(s : T_4)$.
- Case (VT-MutTop): $T_1 = \{\mathsf{M}(r_0) : \bot..\top\}$. Directly by (VT-MutTop).
- Case (VT-AndI): $T_1 = T_4 \wedge T_5$, and $\Gamma_1, \Gamma_2;\rho \vdash x : T_4$, and $\Gamma_1, \Gamma_2;\rho \vdash x : T_5$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : T_4$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : T_5$. By (VT-AndI), $\Gamma_1, x_2 : T_2, \Gamma_2; \rho \vdash x : T_1$.
- Case (VT-Sub): $\Gamma_1, \Gamma_2;\rho \vdash x : T_4$. $\Gamma_1, \Gamma_2;\rho \vdash T_4 <: T_1$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : T_4$. By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_4 <: T_1$. By (VT-Sub), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : T_1$.
- Cases (ST-Top), (ST-Bot), (ST-Refl), (ST-Eq), (ST-N-Rec), (ST-N-Fld), (ST-N-Typ), (ST-N-Met), (ST-N-M), (ST-And1), (ST-And2), (ST-Or1), (ST-Or2), (ST-TypAnd), (ST-Dist): Rules are independent on $\Gamma$, so they apply the same.
- Case (ST-And): $T_1 = T_4 \wedge T_5$, and $\Gamma_1, \Gamma_2;\rho \vdash T_3 <: T_4$, and $\Gamma_1, \Gamma_2;\rho \vdash T_3 <: T_5$. By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3 <: T_4$, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3 <: T_5$. By (ST-And), $\Gamma_1, x_2 : T_2, \Gamma_2; \rho \vdash T_3 <: T_4 \wedge T_5$.
- Case (ST-Or): $T_3 = T_4 \vee T_5$, and $\Gamma_1, \Gamma_2;\rho \vdash T_4 <: T_1$, and $\Gamma_1, \Gamma_2;\rho \vdash T_5 <: T_1$. By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_4 <: T_1$, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_5 <: T_1$. By (ST-Or), $\Gamma_1, x_2 : T_2, \Gamma_2; \rho \vdash T_4 \vee T_5 <: T_1$.

- Case (ST-Trans): $\Gamma_1, \Gamma_2;\rho \vdash T_3 <: T_4$, and $\Gamma_1, \Gamma_2;\rho \vdash T_4 <: T_1$.

  By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3 <: T_4$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_4 <: T_1$. By (ST-Trans), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3 <: T_1$.

- Case (ST-Fld): $T_3 = \{a : T_4..T_5\}$, and $T_1 = \{a : T_6..T_7\}$, where $\Gamma_1, \Gamma_2;\rho \vdash T_6 <: T_4$, and $\Gamma_1, \Gamma_2;\rho \vdash T_5 <: T_7$.

  By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_6 <: T_4$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_5 <: T_7$. By (ST-Fld).

- Case (ST-Typ): $T_3 = \{B(r) : T_4..T_5\}$, and $T_1 = \{B(r) : T_6..T_7\}$, where $\Gamma_1, \Gamma_2;\rho \vdash T_6 <: T_4$, and $\Gamma_1, \Gamma_2;\rho \vdash T_5 <: T_7$.

  By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_6 <: T_4$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_5 <: T_7$. By (ST-Typ).

- Case (ST-Met): $T_3 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, where $\Gamma_1, \Gamma_2;\rho \vdash T_7 <: T_4$, and $\Gamma_1, \Gamma_2, z : T_7;\rho \vdash T_9 <: T_6$, and $\Gamma_1, \Gamma_2, z : T_7, r : T_9;\rho \vdash T_5 <: T_8$. Using alpha-equivalence, assume that $x_2$ is disjoint from $z$ and $r$.

  By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_7 <: T_4$. By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2, z : T_7;\rho \vdash T_9 <: T_6$, and $\Gamma_1, x_2 : T_2, \Gamma_2, z : T_7, r : T_9;\rho \vdash T_5 <: T_8$. By (ST-Met).

- Case (ST-SelU): $T_3 = x_3.B(x_4)$, and $T_1 = [x_4/r]T_5$, and $\Gamma_1, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$.

  By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$. By (ST-SelU), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3.B(x_4) <: [x_4/r]T_5$.

- Case (ST-SelL): $T_3 = [x_4/r]T_4$, and $T_1 = x_3.B(x_4)$, and $\Gamma_1, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$.

  Similarly as (ST-SelU). By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$. By (ST-SelL), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash [x_4/r]T_4 <: x_3.B(x_4)$.

- Cases (TS-Top), (TS-Bot), (TS-M), (TS-Typ), (TS-Met), (TS-Fld), (TS-Rec): Rules do not depend on $\Gamma$, so they apply the same.

- Case (TS-Sel): $T_3 = x_3.B(x_4)$. $\Gamma_1, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_5..T_6\}$. $\Gamma_1, \Gamma_2;\rho \vdash [x_4/r]T_6 \textbf{ ro } T_1$. $\Gamma_1, \Gamma_2;\rho \vdash [x_4/r]T_6 \textbf{ mu}(r_1)\ T_4$.

  By induction on variable typing and splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_5..T_6\}$, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash [x_4/r]T_6 \textbf{ ro } T_1$, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash [x_4/r]T_6 \textbf{ mu}(r_1)\ T_4$. By (TS-Sel), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3.B(x_4) \textbf{ ro } T_1$, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3.B(x_4) \textbf{ mu}(r_1)\ T_4$.

- Case (TS-AndR): $T_3 = T_5 \wedge T_6$, and $T_1 = T_7 \wedge T_8$, where $\Gamma_1, \Gamma_2;\rho \vdash T_5 \textbf{ ro } T_7$, and $\Gamma_1, \Gamma_2;\rho \vdash T_6 \textbf{ ro } T_8$.

  By induction on splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_5 \textbf{ ro } T_7$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_6 \textbf{ ro } T_8$. By (TS-AndR).

- Case (TS-AndM): $T_3 = T_5 \wedge T_6$, and $T_4 = T_7 \wedge T_8$, where $\Gamma_1, \Gamma_2;\rho \vdash T_5 \textbf{ mu}(r_1)\ T_7$, and $\Gamma_1, \Gamma_2;\rho \vdash T_6 \textbf{ mu}(r_1)\ T_8$.

  By induction on splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_5 \textbf{ mu}(r_1)\ T_7$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_6 \textbf{ mu}(r_1)\ T_8$. By (TS-AndM).

- Case (TS-OrR): $T_3 = T_5 \vee T_6$, and $T_1 = T_7 \vee T_8$, where $\Gamma_1, \Gamma_2;\rho \vdash T_5 \textbf{ ro } T_7$, and $\Gamma_1, \Gamma_2;\rho \vdash T_6 \textbf{ ro } T_8$.

  By induction on splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_5 \textbf{ ro } T_7$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_6 \textbf{ ro } T_8$. By (TS-OrR).

- Case (TS-OrM): $T_3 = T_5 \vee T_6$, and $T_4 = T_7 \vee T_8$, where $\Gamma_1, \Gamma_2;\rho \vdash T_5 \textbf{ mu}(r_1)\ T_7$, and $\Gamma_1, \Gamma_2;\rho \vdash T_6 \textbf{ mu}(r_1)\ T_8$.

  By induction on splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_5 \textbf{ mu}(r_1)\ T_7$, and $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_6 \textbf{ mu}(r_1)\ T_8$. By (TS-OrM).

- Case (TT-Var): $t = \mathsf{v}x$, and $\Gamma_1, \Gamma_2;\rho \vdash x : T_1$, and $\Gamma_1, \Gamma_2 \textbf{ vis } x$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x : T_1$. By induction on visibility, $\Gamma_1, x_2 : T_2, \Gamma_2 \textbf{ vis } x$. By (TT-Var), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash \mathsf{v}x : T_1$.

- Case (TT-Apply): $t = x_3.m\, x_4$. $T_1 = [x_3/r][x_4/z]T_4$. $\Gamma_1, \Gamma_2;\rho \vdash x_3 : \{m(z : T_3, r : T_5) : T_4\}$. $\Gamma_1, \Gamma_2;\rho \vdash x_4 : T_3$. $\Gamma_1, \Gamma_2;\rho \vdash x_3 : [x_4/z]T_5$. $\Gamma_1, \Gamma_2 \textbf{ vis } x_3$. $\Gamma_1, \Gamma_2 \textbf{ vis } x_4$.

  Using alpha-equivalence, assume that $x_2$ is disjoint from $z$ and $r$.

By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3 : \{m(z : T_3, r : T_5) : T_4\}$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_4 : T_3$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2; \rho \vdash x_3 : [x_4/z]T_5$. By induction on visibility, $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x_3$, and $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x_4$. By (TT-Apply), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : [x_3/r][x_4/z]T_4$.

- Case (TT-Read): $t = x_3.a$. $T_1 = T_5 \wedge \{\mathsf{M}(r_0) : \bot..(T_6 \vee x_3.\mathsf{M}(r_0))\}$. $\Gamma_1, \Gamma_2;\rho \vdash x_3 : \{a : T_3..T_4\}$. $\Gamma_1, \Gamma_2;\rho \vdash T_4$ **ro** $T_5$. $\Gamma_1, \Gamma_2;\rho \vdash T_4$ $\mathbf{mu}(r_0)$ $T_6$. $\Gamma_1, \Gamma_2$ **vis** $x_3$.

  By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3 : \{a : T_3..T_4\}$. By induction on splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_4$ **ro** $T_5$. By induction on splitting, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_4$ $\mathbf{mu}(r_0)$ $T_6$. By induction on visibility, $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x_3$. By (TT-Read), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : T_5 \wedge \{\mathsf{M}(r_0) : \bot..(T_6 \vee x_3.\mathsf{M}(r_0))\}$.

- Case (TT-Write): $t = x_3.a := x_4$. $\Gamma_1, \Gamma_2;\rho \vdash x_4 : T_3$. $\Gamma_1, \Gamma_2;\rho \vdash x_3 : \{a : T_3..T_1\}$. $\Gamma_1, \Gamma_2;\rho \vdash x_3 : \{\mathsf{M}(r_0) : \bot..\bot\}$. $\Gamma_1, \Gamma_2$ **vis** $x_3$. $\Gamma_1, \Gamma_2$ **vis** $x_4$.

  By induction on visibility, $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x_3$, and $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x_4$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_4 : T_3$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2; \rho \vdash x_3 : \{a : T_3..T_1\}$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash x_3 : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (TT-Write), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : T_1$.

- Case (TT-New): $t = \mathsf{let}\ z = \nu(s : T_3)d\ \mathsf{in}\ t_1$. $\Gamma_1, \Gamma_2, s : T_3;\rho \vdash d : T_3$. $\Gamma_1, \Gamma_2, z : \mu(s : T_3) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash t_1 : T_1$. $z \notin \text{fv}\ T_1$. $T_3$ **indep** $s$.

  Using alpha-equivalence, assume that $x_2$ is disjoint from $s$ and $z$.

  By induction on definition typing, $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3;\rho \vdash d : T_3$. By induction on term typing, $\Gamma_1, x_2 : T_2, \Gamma_2, z : \mu(s : T_3) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash t_1 : T_1$. By (TT-New), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : T_1$.

- Case (TT-Let): $t = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$, where $\Gamma_1, \Gamma_2;\rho \vdash t_1 : T_3$, and $\Gamma_1, \Gamma_2, z : T_3;\rho \vdash t_2 : T_1$, and $z \notin \text{fv}\ T_1$.

  Using alpha-equivalence, assume that $x_2$ is distinct from $z$.

  By induction on term typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t_1 : T_3$. By induction on term typing, $\Gamma_1, x_2 : T_2, \Gamma_2, z : T_3;\rho \vdash t_2 : T_1$. By (TT-Let), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : T_1$.

- Case (TT-Sub): $\Gamma_1, \Gamma_2;\rho \vdash t : T_3$, and $\Gamma_1, \Gamma_2;\rho \vdash T_3 <: T_1$. By induction on term typing, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : T_3$. By induction on subtyping, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3 <: T_1$. By (TT-Sub), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash t : T_1$.

- Cases (DT-Typ), (DT-TypB), (HT-Typ), (HT-TypB): Rules do not depend on $\Gamma$, so they apply the same.

- Case (DT-Fld): $d = \{a = x_3\}$, and $T_1 = \{a : T_4..T_4\}$, where $\Gamma_1, \Gamma_2, s : T_3$ **vis** $x_3$, and $\Gamma_1, \Gamma_2, s : T_3; \rho \vdash x_3 : T_4$.

  By induction on visibility, $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3$ **vis** $x_3$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3;\rho \vdash x_3 : T_4$. By (DT-Fld), $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3;\rho \vdash \{a = x_3\} : \{a : T_4..T_4\}$.

- Case (HT-Fld): $d = \{a = x_3\}$, and $T_1 = \{a : T_4..T_4\}$, where $\Gamma_1, \Gamma_2$ **vis** $x_3$, and $\Gamma_1, \Gamma_2;\rho \vdash x_3 : T_4$.

  By induction on visibility, $\Gamma_1, x_2 : T_2, \Gamma_2$ **vis** $x_3$. By induction on variable typing, $\Gamma_1, x_2 : T_2, \Gamma_2; \rho \vdash x_3 : T_4$. By (HT-Fld), $\Gamma_1, x_2 : T_2, \Gamma_2, y/s : T_3;\rho \vdash \{a = x_3\} : \{a : T_4..T_4\}$.

- Case (DT-And): $d = d_1 \wedge d_2$, and $T_1 = T_4 \wedge T_5$, where $\Gamma_1, \Gamma_2, s : T_3;\rho \vdash d_1 : T_4$, and $\Gamma_1, \Gamma_2, s : T_3; \rho \vdash d_2 : T_5$, and $d_1$ and $d_2$ have distinct member names.

  By induction on definition typing, $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3;\rho \vdash d_1 : T_4$, and $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3; \rho \vdash d_2 : T_5$. By (DT-And), $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3;\rho \vdash d_1 \wedge d_2 : T_4 \wedge T_5$.

- Case (HT-And): $d = d_1 \wedge d_2$, and $T_1 = T_4 \wedge T_5$, where $\Gamma_1, \Gamma_2, y/s : T_3;\rho \vdash d_1 : T_4$, and $\Gamma_1, \Gamma_2, y/s : T_3; \rho \vdash d_2 : T_5$, and $d_1$ and $d_2$ have distinct member names.

  By induction on definition typing, $\Gamma_1, x_2 : T_2, \Gamma_2, y/s : T_3;\rho \vdash d_1 : T_4$, and $\Gamma_1, x_2 : T_2, \Gamma_2, y/s : T_3; \rho \vdash d_2 : T_5$. By (HT-And), $\Gamma_1, x_2 : T_2, \Gamma_2, y/s : T_3;\rho \vdash d_1 \wedge d_2 : T_4 \wedge T_5$.

- Case (DT-Met): $d = \{m(z, r) = t\}$, and $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, where $\Gamma_1, \Gamma_2, s : T_3, !, z : T_4, r : T_3 \wedge [r/s]T_3 \wedge T_6;\rho \vdash t : T_5$, and $z \notin \text{fv}\ T_4 \cup \text{fv}\ T_3$, and $r \notin \text{fv}\ T_4 \cup \text{fv}\ T_6 \cup \text{fv}\ T_3$. Using alpha-equivalence, assume that $x_2$ is disjoint from $z$ and $r$.

  By induction on term typing, $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3, !, z : T_4, r : T_3 \wedge [r/s]T_3 \wedge T_6;\rho \vdash t : T_5$. By (DT-Met), $\Gamma_1, x_2 : T_2, \Gamma_2, s : T_3;\rho \vdash \{m(z, r) = t\} : \{m(z : T_4, r : T_6) : T_5\}$.

- Case (HT-Met): $d = \{m(z,r) = t\}$, and $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, where $\Gamma_1, \Gamma_2, !, z : T_4, r : [y/s]T_3 \wedge [r/s]T_3 \wedge T_6;\rho \vdash t : T_5$, and $z \notin \text{fv } T_4 \cup \text{fv } T_3$, and $r \notin \text{fv } T_4 \cup \text{fv } T_6 \cup \text{fv } T_3$. Using alpha-equivalence, assume that $x_2$ is disjoint from $z$ and $r$.

  By induction on term typing, $\Gamma_1, x_2 : T_2, \Gamma_2, !, z : T_4, r : [y/s]T_3 \wedge [r/s]T_3 \wedge T_6;\rho \vdash t : T_5$. By (HT-Met), $\Gamma_1, x_2 : T_2, \Gamma_2, y/s : T_3;\rho \vdash \{m(z,r) = t\} : \{m(z : T_4, r : T_6) : T_5\}$.

□

**Lemma 5.6** (WknS)**.** *If* $\Gamma_1, \Gamma_2;\rho \vdash \sigma : T_3, T_1$*, and* $\Gamma_1, x_2 : T_2, \Gamma_2$ *is inert, then* $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash \sigma : T_3, T_1$.

*Idea.* Adding variables to a context preserves stack typing ▽

*Proof.* Because $\Gamma_1, x_2 : T_2, \Gamma_2$ is inert, then $x_2 \notin \text{dom } \Gamma_1, \Gamma_2$. Induction on $\Gamma_1, \Gamma_2;\rho \vdash \sigma : T_3, T_1$:

- Case (CT-EmptyS): $\Gamma_1, \Gamma_2;\rho \vdash T_3 <: T_1$, and $\sigma = \cdot$. By 5.5(Wkn), $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash T_3 <: T_1$. By (CT-EmptyS).
- Case (CT-LetS): $\sigma = \sigma_1 :: \mathsf{let}\ z = \square\ \mathsf{in}\ t$. $\Gamma_1, \Gamma_2;\rho \vdash \sigma_1 : T_4, T_1$. $\Gamma_1, \Gamma_2, z : T_3;\rho \vdash t : T_4$. $z \notin \text{fv } T_4$.

  Using alpha-equivalence, assume that $x_2$ is distinct from $z$.

  By induction, $\Gamma_1, x_2 : T_2, \Gamma_2;\rho \vdash \sigma_1 : T_4, T_1$. By 5.5(Wkn), $\Gamma_1, x_2 : T_2, \Gamma_2, z : T_3;\rho \vdash t : T_4$. By (CT-LetS).

□

**Lemma 5.7** (WknE)**.** *If* $\mathrm{F}_1, \mathrm{F}_2 \sim \rho$*, and* $\mathrm{F}_1, v : T_2, \mathrm{F}_2$ *is inert, then* $\mathrm{F}_1, v : T_2, \mathrm{F}_2 \sim \rho$.

*Idea.* Adding variables to a context preserves environment correspondence ▽

*Proof.* Because $\mathrm{F}_1, v : T_2, \mathrm{F}_2$ is inert, then $v \notin \text{dom } \mathrm{F}_1, \mathrm{F}_2$. Induction on $\mathrm{F}_1, \mathrm{F}_2 \sim \rho$:

- Case (CT-EmptyE): $\rho = \cdot$. Directly by (CT-EmptyE).
- Case (CT-RefE): $\rho = \rho_1, w \to y$, and $\mathrm{F}_3 \sim \rho_1$, and $\mathrm{F}_1, \mathrm{F}_2 = \mathrm{F}_3, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_4, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_3\}, \mathrm{F}_5$.

  Because $v \notin \text{dom } \mathrm{F}_1, \mathrm{F}_2$, then $v \neq w$, and $v \neq y$. $v$ is added into $\mathrm{F}_3$, $\mathrm{F}_4$ or $\mathrm{F}_5$. If $v$ is added into $\mathrm{F}_3$, then by induction. By (CT-RefE), which applies the same.

□

Similarly to weakening lemmata, where the typing context is extended by a new variable, we show that when the runtime environment is extended, then equivalence, various kinds of typing, subtyping and splitting are also preserved.

**Lemma 5.8** (EWkn)**.** *The following holds for typing, subtyping and splitting:*

- *If* $\rho \vdash T_3 \approx T_1$*, then* $\rho, w \to y \vdash T_3 \approx T_1$.
- *If* $\Gamma;\rho \vdash x : T_1$*, then* $\Gamma;\rho, w \to y \vdash x : T_1$.
- *If* $\Gamma;\rho \vdash T_3 <: T_1$*, then* $\Gamma;\rho, w \to y \vdash T_3 <: T_1$.
- *If* $\Gamma;\rho \vdash T_3\ \mathbf{ro}\ T_1$*, then* $\Gamma;\rho, w \to y \vdash T_3\ \mathbf{ro}\ T_1$.
- *If* $\Gamma;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$*, then* $\Gamma;\rho, w \to y \vdash T_3\ \mathbf{mu}(r_1)\ T_4$.
- *If* $\Gamma;\rho \vdash t : T_1$*, then* $\Gamma;\rho, w \to y \vdash t : T_1$.
- *If* $\Gamma, s : T_3;\rho \vdash d : T_1$*, then* $\Gamma, s : T_3;\rho, w \to y \vdash d : T_1$.
- *If* $\Gamma, y/s : T_3;\rho \vdash d : T_1$*, then* $\Gamma, y/s : T_3;\rho, w \to y \vdash d : T_1$.

*Proof idea.* Straightforward induction on variable typing, term typing, definition typing, type equivalence, subtyping and splitting. ▽

*Proof.* Induction on variable typing, term typing, definition typing, type equivalence, subtyping and splitting:

- Case (VE-RtoL): If $v_1 \to v_2 \in \rho$, then $v_1 \to v_2 \in \rho, w \to y$. Use the same rule.
- All other cases use $\rho$ in premises only directly in typing, equivalence, subtyping or splitting. By induction, show the same for $\rho, w \to y$, then use the same rule.

□

**Lemma 5.9** (EWknS)**.** *If* $\Gamma;\rho \vdash \sigma : T_3, T_1$, *then* $\Gamma;\rho, w \to y \vdash \sigma : T_3, T_1$.

*Idea.* Adding to the runtime environment preserves stack typing ▽

*Proof.* $\Gamma$ is inert. Induction on $\Gamma;\rho \vdash \sigma : T_3, T_1$:

- Case (CT-EmptyS): $\Gamma;\rho \vdash T_3 <: T_1$, and $\sigma = \cdot$. By 5.8(EWkn), $\Gamma;\rho, w \to y \vdash T_3 <: T_1$. By (CT-EmptyS).
- Case (CT-LetS): $\sigma = \sigma_1 :: \mathsf{let}\ z = \square\ \mathsf{in}\ t$. $\Gamma;\rho \vdash \sigma_1 : T_4, T_1$. $\Gamma, z : T_3;\rho \vdash t : T_4$. $z \notin \text{fv}\ T_4$.

  By induction, $\Gamma;\rho, w \to y \vdash \sigma_1 : T_4, T_1$. By 5.8(EWkn), $\Gamma, z : T_3;\rho, w \to y \vdash t : T_4$. By (CT-LetS).

□

For heap correspondence, we state three variants of weakening: appending a location to the context, and appending a reference to both the context and the environment for partial and for full heap correspondence.

**Lemma 5.10** (WknHL)**.** *If* $\mathrm{F}_1;\rho \vdash \mathrm{F}_2 \sim \Sigma$, *and* $\mathrm{F}_1, y : T$ *is inert, then* $\mathrm{F}_1, y : T;\rho \vdash \mathrm{F}_2 \sim \Sigma$.

*Idea.* Adding a location to an inert context preserves correspondence of a part of a heap. ▽

*Proof idea.* Induction on heap part correspondence, using weakening on object typing. ▽

*Proof.* Because $\mathrm{F}_1, y : T$ is inert, then $y \notin \text{dom}\ \mathrm{F}_1$. Induction on $\mathrm{F}_1;\rho \vdash \mathrm{F}_2 \sim \Sigma$:

- Case (CT-EmptyH): Directly by (CT-EmptyH) (does not depend on $\mathrm{F}_1$).
- Case (CT-ObjH): $\mathrm{F}_2 = \mathrm{F}_3, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. $\Sigma = \Sigma_3, y_1 \to d$. $\mathrm{F}_1;\rho \vdash \mathrm{F}_3 \sim \Sigma_3$. $\mathrm{F}_1, y_1/s : R;\rho \vdash d : [y_1/s]R$. $R$ **indep** $s$.

  By induction, $\mathrm{F}_1, y : T;\rho \vdash \mathrm{F}_3 \sim \Sigma_3$. By 5.5(Wkn), $\mathrm{F}_1, y : T, y_1/s : R;\rho \vdash d : [y_1/s]R$. By (CT-ObjH), $\mathrm{F}_1, y : T;\rho \vdash \mathrm{F}_2 \sim \Sigma$.
- Case (CT-RefH): $\mathrm{F}_2 = \mathrm{F}_3, w_1 : T$. $\mathrm{F}_1;\rho \vdash \mathrm{F}_3 \sim \Sigma$.

  By induction, $\mathrm{F}_1, y : T;\rho \vdash \mathrm{F}_3 \sim \Sigma$. By (CT-RefH), $\mathrm{F}_1, y : T;\rho \vdash \mathrm{F}_2 \sim \Sigma$.

□

**Lemma 5.11** (WknHP)**.** *If* $\mathrm{F}_1;\rho \vdash \mathrm{F}_2 \sim \Sigma$, *and* $\mathrm{F}_1, w : T$ *is inert, then* $\mathrm{F}_1, w : T;\rho, w \to y \vdash \mathrm{F}_2 \sim \Sigma$.

*Idea.* Adding a reference to an inert context preserves correspondence of a part of a heap. ▽

*Proof idea.* Induction on heap part correspondence, using weakening on object typing. ▽

*Proof.* Because $\mathrm{F}_1, w : T$ is inert, then $w \notin \text{dom}\ \mathrm{F}_1$. Induction on $\mathrm{F}_1;\rho \vdash \mathrm{F}_2 \sim \Sigma$:

- Case (CT-EmptyH): Directly by (CT-EmptyH) (does not depend on $\mathrm{F}_1$).
- Case (CT-ObjH): $\mathrm{F}_2 = \mathrm{F}_3, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. $\Sigma = \Sigma_3, y_1 \to d$. $\mathrm{F}_1;\rho \vdash \mathrm{F}_3 \sim \Sigma_3$. $\mathrm{F}_1, y_1/s : R;\rho \vdash d : [y_1/s]R$. $R$ **indep** $s$.

  By induction, $\mathrm{F}_1, w : T;\rho, w \to y \vdash \mathrm{F}_3 \sim \Sigma_3$. By 5.5(Wkn), $\mathrm{F}_1, w : T, y_1/s : R;\rho \vdash d : [y_1/s]R$. By 5.8(EWkn), $\mathrm{F}_1, w : T, y_1/s : R;\rho, w \to y \vdash d : [y_1/s]R$. By (CT-ObjH), $\mathrm{F}_1, w : T;\rho, w \to y \vdash \mathrm{F}_2 \sim \Sigma$.
- Case (CT-RefH): $\mathrm{F}_2 = \mathrm{F}_3, w_1 : T$. $\mathrm{F}_1;\rho \vdash \mathrm{F}_3 \sim \Sigma$.

  By induction, $\mathrm{F}_1, w : T;\rho, w \to y \vdash \mathrm{F}_3 \sim \Sigma$. By (CT-RefH), $\mathrm{F}_1, w : T;\rho, w \to y \vdash \mathrm{F}_2 \sim \Sigma$.

□

**Lemma 5.12** (WknH)**.** *If* $\mathrm{F};\rho \sim \Sigma$, *and* $\mathrm{F}, w : T$ *is inert, then* $\mathrm{F}, w : T;\rho, w \to y \sim \Sigma$.

*Idea.* Adding a reference to an inert context preserves heap correspondence. ▽

*Proof idea.* The heap correspondece rules allow any assignment of types to references and do not depend on them. ▽

*Proof.* By inversion of (CT-CorrH), $\mathrm{F};\rho \vdash \mathrm{F} \sim \Sigma$, and all fields in $\Sigma$ are locations. By 5.11(WknHP), $\mathrm{F}, w : T;\rho, w \to y \vdash \mathrm{F} \sim \Sigma$. By (CT-RefH), $\mathrm{F}, w : T;\rho, w \to y \vdash \mathrm{F}, w : T \sim \Sigma$. By (CT-CorrH), $\mathrm{F}, w : T;$ $\rho, w \to y \sim \Sigma$. □

The narrowing lemma states that if a type in a typing context is replaced by a subtype, then typing is preserved.

**Lemma 5.13** (Narr)**.** *The following holds for typing and subtyping:*

- *If* $\Gamma_1, u : T_4, \Gamma_2$ **vis** $x$*, and* $\Gamma_1;\rho \vdash T_2 <: T_4$*, then* $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x$.
- *If* $\Gamma_1, u : T_4, \Gamma_2;\rho \vdash x : T_1$*, and* $\Gamma_1;\rho \vdash T_2 <: T_4$*, then* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x : T_1$.
- *If* $\Gamma_1, u : T_4, \Gamma_2;\rho \vdash T_3 <: T_1$*, and* $\Gamma_1;\rho \vdash T_2 <: T_4$*, then* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3 <: T_1$.
- *If* $\Gamma_1, u : T_4, \Gamma_2;\rho \vdash T_3\ \mathbf{ro}\ T_1$*, and* $\Gamma_1;\rho \vdash T_2 <: T_4$*, then* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3\ \mathbf{ro}\ T_1$.
- *If* $\Gamma_1, u : T_4, \Gamma_2;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$*, and* $\Gamma_1;\rho \vdash T_2 <: T_4$*, then* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$.
- *If* $\Gamma_1, u : T_4, \Gamma_2;\rho \vdash t : T_1$*, and* $\Gamma_1;\rho \vdash T_2 <: T_4$*, then* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash t : T_1$.
- *If* $\Gamma_1, u : T_4, \Gamma_2, s : T_3;\rho \vdash d : T_1$*, and* $\Gamma_1;\rho \vdash T_2 <: T_4$*, then* $\Gamma_1, u : T_2, \Gamma_2, s : T_3;\rho \vdash d : T_1$.

*Proof.* Induction on variable typing, term typing, definition typing, subtyping and splitting:

- Case (VT-Var), $x = u$: By (VT-Var) and (VT-Sub).
- Other cases by induction as in 5.5(Wkn).

□

Finally, lemma 5.14(Unhide) shows that removing ! from a typing context preserves typing.

**Lemma 5.14** (Unhide)**.** *The following holds for typing and subtyping:*

- *If* $\Gamma_1, !, \Gamma_2$ **vis** $x$*, then* $\Gamma_1, \Gamma_2$ **vis** $x$.
- *If* $\Gamma_1, !, \Gamma_2;\rho \vdash x : T_1$*, then* $\Gamma_1, \Gamma_2;\rho \vdash x : T_1$.
- *If* $\Gamma_1, !, \Gamma_2;\rho \vdash T_3 <: T_1$*, then* $\Gamma_1, \Gamma_2;\rho \vdash T_3 <: T_1$.
- *If* $\Gamma_1, !, \Gamma_2;\rho \vdash T_3\ \mathbf{ro}\ T_1$*, then* $\Gamma_1, \Gamma_2;\rho \vdash T_3\ \mathbf{ro}\ T_1$.
- *If* $\Gamma_1, !, \Gamma_2;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$*, then* $\Gamma_1, \Gamma_2;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$.
- *If* $\Gamma_1, !, \Gamma_2;\rho \vdash t : T_1$*, then* $\Gamma_1, \Gamma_2;\rho \vdash t : T_1$.
- *If* $\Gamma_1, !, \Gamma_2, s : T_3;\rho \vdash d : T_1$*, then* $\Gamma_1, \Gamma_2, s : T_3;\rho \vdash d : T_1$.

*Idea.* Removing ! from a context preserves typing. ▽

*Proof idea.* Induction on variable typing, term typing, definition typing, subtyping and splitting: ▽

*Proof.* By induction as in 5.5(Wkn). Removing ! does not affect application of any rule. □

### 5.1.3 Environment correspondence lemmata

This section contains lemmata about runtime environment correspondence $\mathrm{F} \sim \rho$. If $w \to y \in \rho$, then in a corresponding context, $w$ and $y$ have the same type except mutability. This is stated in three variants, for when none of the types or one of them is known.

**Lemma 5.15** (ECorrInv)**.** *If* $\Gamma \sim \rho$*, and* $w \to y \in \rho$*, then there exist* $T_2$*,* $\Gamma_1$*,* $\Gamma_2$*,* $\Gamma_3$*,* $\Gamma_4$*,* $s$*,* $R$*, such that* $\Gamma = \Gamma_1, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \Gamma_2$*, and* $\Gamma_1 = \Gamma_3, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_4$*.*

*Idea.* Location and reference have the same, except for mutability. ▽

*Proof idea.* Induction on environment correspondence. ▽

*Proof.* Induction on $\Gamma \sim \rho$:

- Case (CT-EmptyE): Not possible.
- Case (CT-RefE): $\rho = \rho_1, w_1 \to y_1$. $\Gamma = \Gamma_5, w_1 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_3\}, \Gamma_6$. $\Gamma_5 = \Gamma_7, y_1 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_8$. $\Gamma_5 \sim \rho_1$.
  - If $w = w_1$, then choose $T_2 = T_3$, and $s = s_1$, and $R = R_1$, and $\Gamma_3 = \Gamma_7$, and $\Gamma_4 = \Gamma_8$, and $\Gamma_6 = \Gamma_2$, and $\Gamma_5 = \Gamma_1$.
  - Otherwise, $w \neq w_1$, therefore $w \to y \in \rho_1$. By induction, exist $T_2$, $\Gamma_1$, $\Gamma_9$, $\Gamma_3$, $\Gamma_4$, $s$, $R$, such that $\Gamma_5 = \Gamma_1, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \Gamma_9$, and $\Gamma_1 = \Gamma_3, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_4$. Choose $\Gamma_2 = \Gamma_9, w_1 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_3\}, \Gamma_6$, therefore $\Gamma = \Gamma_1, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \Gamma_2$.

□

**Lemma 5.16** (ECorrInvY)**.** *If* $\Gamma \sim \rho$*, and* $w \to y \in \rho$*, and* $\Gamma = \Gamma_1, w : T_1, \Gamma_2$*, then there exist* $T_2$*,* $s$*,* $R$*,* $\Gamma_3$*,* $\Gamma_4$*, such that* $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}$*, and* $\Gamma_1 = \Gamma_3, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_4$*.*

*Idea.* Location has the same type as the reference, except for mutability. ▽

*Proof idea.* By 5.15(ECorrInv) and by uniqueness of variables bound in a context. ▽

*Proof.* By 5.15(ECorrInv), exist $T_2$, $\Gamma_5$, $\Gamma_6$, $\Gamma_3$, $\Gamma_4$, such that $\Gamma = \Gamma_5, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \Gamma_6$, and $\Gamma_5 = \Gamma_3, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_4$. Because we assume that variables bound in context are unique, therefore $\Gamma_1 = \Gamma_5$, and $\Gamma_2 = \Gamma_6$, and $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}$. □

**Lemma 5.17** (ECorrInvW)**.** *If* $\Gamma \sim \rho$*, and* $w \to y \in \rho$*, and* $\Gamma = \Gamma_1, y : T_1, \Gamma_2$*, then there exist* $T_2$*,* $s$*,* $R$*,* $\Gamma_3$*,* $\Gamma_4$*, such that* $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$*, and* $\Gamma_2 = \Gamma_3, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \Gamma_4$*.*

*Idea.* Reference has the same type as the location, except for mutability. ▽

*Proof idea.* Induction on environment correspondence. ▽

*Proof.* By 5.15(ECorrInv), exist $T_2$, $\Gamma_5$, $\Gamma_6$, $\Gamma_3$, $\Gamma_4$, such that $\Gamma = \Gamma_5, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \Gamma_4$, and $\Gamma_5 = \Gamma_6, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_3$. Because we assume that variables bound in context are unique, therefore $\Gamma_1 = \Gamma_6$, therefore $\Gamma_2 = \Gamma_3, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \Gamma_4$, and $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}$. □

### 5.1.4 Subtyping lemmata

This section contains simple helper lemmata about subtyping. The subtyping rules for intersection and union types are stated in a way where the intersection or union type is on one side. With transitivity, it is easy to show subtyping between two intersection and between two union types.

**Lemma 5.18** (AndSub). *If* $\Gamma;\rho \vdash T_1 <: T_3$*, and* $\Gamma;\rho \vdash T_2 <: T_4$*, then* $\Gamma;\rho \vdash T_1 \wedge T_2 <: T_3 \wedge T_4$.

*Idea.* Subtyping between two intersection types. ▽

*Proof.* By (ST-And1), $\Gamma;\rho \vdash T_1 \wedge T_2 <: T_1$, by (ST-Trans), $\Gamma;\rho \vdash T_1 \wedge T_2 <: T_3$. By (ST-And2), $\Gamma;\rho \vdash T_1 \wedge T_2 <: T_2$, by (ST-Trans), $\Gamma;\rho \vdash T_1 \wedge T_2 <: T_4$. By (ST-And), $\Gamma;\rho \vdash T_1 \wedge T_2 <: T_3 \wedge T_4$. □

**Lemma 5.19** (OrSub). *If* $\Gamma;\rho \vdash T_1 <: T_3$*, and* $\Gamma;\rho \vdash T_2 <: T_4$*, then* $\Gamma;\rho \vdash T_1 \vee T_2 <: T_3 \vee T_4$.

*Idea.* Subtyping between two union types. ▽

*Proof.* By (ST-Or1), $\Gamma;\rho \vdash T_3 <: T_3 \vee T_4$, by (ST-Trans), $\Gamma;\rho \vdash T_1 <: T_3 \vee T_4$. By (ST-Or2), $\Gamma;\rho \vdash T_4 <: T_3 \vee T_4$, by (ST-Trans), $\Gamma;\rho \vdash T_2 <: T_3 \vee T_4$. By (ST-Or), $\Gamma;\rho \vdash T_1 \vee T_2 <: T_3 \vee T_4$. □

The next lemma shows subtyping between an union and a type member declaration.

**Lemma 5.20** (OrTypSub). *If* $\Gamma;\rho \vdash T_1 <: \{B(r) : T_2..T_3\}$*, and* $\Gamma;\rho \vdash T_4 <: \{B(r) : T_5..T_6\}$*, then* $\Gamma;\rho \vdash T_1 \vee T_4 <: T_7$*, where* $T_7 = \{B(r) : T_2 \wedge T_5..T_3 \vee T_6\}$.

*Proof.* By (ST-And1), $\Gamma;\rho \vdash T_2 \wedge T_5 <: T_2$. By (ST-Or1), $\Gamma;\rho \vdash T_3 <: T_3 \vee T_6$. By (ST-Typ), $\Gamma;\rho \vdash \{B(r) : T_2..T_3\} <: T_7$. By (ST-Trans), $\Gamma;\rho \vdash T_1 <: T_7$. By (ST-And2), $\Gamma;\rho \vdash T_2 \wedge T_5 <: T_5$. By (ST-Or2), $\Gamma;\rho \vdash T_6 <: T_3 \vee T_6$. By (ST-Typ), $\Gamma;\rho \vdash \{B(r) : T_5..T_6\} <: T_7$. By (ST-Trans), $\Gamma;\rho \vdash T_4 <: T_7$. By (ST-Or), $\Gamma;\rho \vdash T_1 \vee T_4 <: T_7$. □

### 5.1.5 Substitution Lemmata

This section contains several variants of substitution lemmata, following the form of the substitution lemma in kDOT [2]. The standard case of substituting an abstract variable for another variable in typing relations is stated in 5.27(SubV) and 5.28(SubT).

The lemmata 5.21(SubSwap), 5.22(SubVarNe) and 5.23(SubId) show some simple properties of substitution of variables.

**Lemma 5.21** (SubSwap). *If $x_1 \neq x_3$ and $x_1 \neq x_4$, then the following holds for variable and type substitution:*

- $[x_4/x_3][x_2/x_1]x_0 = [[x_4/x_3]x_2/x_1][x_4/x_3]x_0$
- $[x_4/x_3][x_2/x_1]T = [[x_4/x_3]x_2/x_1][x_4/x_3]T$

.

*Proof.* Will show that if $[x_4/x_3][x_2/x_1]x_0 = x_5$, then $[[x_4/x_3]x_2/x_1][x_4/x_3]x_0 = x_5$. By cases on $[x_4/x_3][x_2/x_1]x_0 = x_5$:

- Case (VX-VarE): $x_3 = [x_2/x_1]x_0$. $x_5 = x_4$. By cases on $x_3 = [x_2/x_1]x_0$:
  - Case (VX-VarE): $x_1 = x_0$. $x_3 = x_2$. Because $x_0 \neq x_3$, by (VX-VarN), $[x_4/x_3]x_0 = x_0 = x_1$. By (VX-VarE), $[x_4/x_3]x_2 = x_5$. By (VX-VarE), $[[x_4/x_3]x_2/x_1]x_1 = x_5$.
  - Case (VX-VarN): $x_1 \neq x_0$. $x_3 = x_0$. By (VX-VarE), $[x_4/x_3]x_0 = x_5$. Because $x_1 \neq x_3$, by (VX-VarN), $[x_4/x_3]x_1 = x_1$. Because $x_1 \neq x_5$, by (VX-VarN), $[[x_4/x_3]x_2/x_1]x_5 = x_5$.
- Case (VX-VarN): $x_3 \neq [x_2/x_1]x_0$. $x_5 = [x_2/x_1]x_0$. By cases on $x_5 = [x_2/x_1]x_0$:
  - Case (VX-VarE): $x_1 = x_0$. $x_5 = x_2$. Because $x_0 \neq x_3$, by (VX-VarN), $[x_4/x_3]x_0 = x_0 = x_1$. Because $x_3 \neq x_5$, we have $x_2 \neq x_3$, so by (VX-VarN), $[x_4/x_3]x_2 = x_2 = x_5$. By (VX-VarE), $[[x_4/x_3]x_2/x_1]x_1 = x_5$.
  - Case (VX-VarN): $x_1 \neq x_0$. $x_5 = x_0$. Because $x_0 \neq x_3$, by (VX-VarN), $[x_4/x_3]x_0 = x_0 = x_5$. Because $x_5 \neq x_1$, by (VX-VarN), $[[x_4/x_3]x_2/x_1]x_5 = x_5$.

Will show that if $[x_4/x_3][x_2/x_1]T = T_2$, then $[[x_4/x_3]x_2/x_1][x_4/x_3]T = T_2$. Induction on $[x_4/x_3][x_2/x_1]T = T_2$:

- All cases directly by induction and the same rule.

□

**Lemma 5.22** (SubVarNe). *If $x_0 \neq x_5$, and $x_2 \neq x_5$, then $[x_2/x_1]x_0 \neq x_5$.*

*Proof.* If $x_0 = x_1$, then by (VX-VarE), $[x_2/x_1]x_0 = x_2 \neq x_5$. If $x_0 \neq x_1$, then by (VX-VarN), $[x_2/x_1]x_0 = x_0 \neq x_5$. □

**Lemma 5.23** (SubId). *If $x_1 \neq x_2$, then the following holds for variable and type substitution:*

- $[x_4/x_1][x_2/x_1]x_0 = [x_2/x_1]x_0$
- $[x_4/x_1][x_2/x_1]T = [x_2/x_1]T$

.

*Proof.*
- If $x_0 = x_1$. By (VX-VarE), $[x_2/x_1]x_0 = x_2$. By (VX-VarN), $[x_4/x_1][x_2/x_1]x_0 = x_2$.
- If $x_0 \neq x_1$. By (VX-VarN), $[x_2/x_1]x_0 = x_0$. By (VX-VarN), $[x_4/x_1][x_2/x_1]x_0 = x_0$.
- For types, by straightforward induction on replacement in types.

□

The lemmata 5.24(SubVis), 5.25(SubIndep) and 5.26(SubEq) show how substitution preserves visibility, independence on mutability and type equivalence.

**Lemma 5.24** (SubVis). *If $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x_1$, and $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x$, then $\Gamma_1, [x/u]\Gamma_2$ **vis** $[x/u]x_1$.*

*Proof.* If $x_1 = u$, then $[x/u]x_1 = x$. Because no ! is added, then $\Gamma_1, [x/u]\Gamma_2$ **vis** $x$. If $x_1 \neq u$, then $[x/u]x_1 = x_1$. Because no ! is added, then $\Gamma_1, [x/u]\Gamma_2$ **vis** $x_1$. □

**Lemma 5.25** (SubIndep)**.** *If $T$ **indep** $s$, and $x \neq s$, then $[x/u]T$ **indep** $s$.*

*Proof.* Induction on $T$ **indep** $s$:

- Case (TI-Top): $T = \top$. By (TX-Top) and (TI-Top).
- Case (TI-Bot): $T = \bot$. By (TX-Bot) and (TI-Bot).
- Case (TI-N): $T = \mathsf{N}$. By (TX-N) and (TI-N).
- Case (TI-And): $T = T_1 \wedge T_2$, and $T_1$ **indep** $s$, and $T_2$ **indep** $s$. By induction, $[x/u]T_1$ **indep** $s$, and $[x/u]T_2$ **indep** $s$. By (TX-And) and (TI-And).
- Case (TI-Or): $T = T_1 \vee T_2$, and $T_1$ **indep** $s$, and $T_2$ **indep** $s$. By induction, $[x/u]T_1$ **indep** $s$, and $[x/u]T_2$ **indep** $s$. By (TX-Or) and (TI-Or).
- Case (TI-SelM): $T = x_1.\mathsf{M}(x_2)$, where $x_1 \neq s$, and $x_2 \neq s$. By 5.22(SubVarNe), $[x/u]x_1 \neq s$, and $[x/u]x_2 \neq s$. By (TI-SelM).
- Case (TI-SelA): $T = x_1.A(x_2)$, where $x_2 \neq s$. By 5.22(SubVarNe), $[x/u]x_2 \neq s$. By (TI-SelA).
- Case (TI-Rec): $T = \mu(s_2 : T_1)$, and $T_1$ **indep** $s$. Using alpha-equivalence, assume that $s \neq s_2$, and $s_2 \neq u$, and $s_2 \neq x$. By induction, $[x/u]T_1$ **indep** $s$. By (TX-Rec), $[x/u]T = \mu(s_2 : [x/u]T_1)$. By (TI-Rec).
- Case (TI-Typ): $T = \{B(r) : T_1..T_2\}$, and $T_1$ **indep** $s$, and $T_2$ **indep** $s$. By induction, $[x/u]T_1$ **indep** $s$, and $[x/u]T_2$ **indep** $s$. By (TX-Typ) and (TI-Typ).
- Case (TI-Fld): $T = \{a : T_1..T_2\}$, and $T_1$ **indep** $s$, and $T_2$ **indep** $s$. By induction, $[x/u]T_1$ **indep** $s$, and $[x/u]T_2$ **indep** $s$. By (TX-Fld) and (TI-Fld).
- Case (TI-Met): $T = \{m(z : T_1, r : T_3) : T_2\}$, and $T_1$ **indep** $s$, and $T_2$ **indep** $s$, and $T_3$ **indep** $s$. By induction, $[x/u]T_1$ **indep** $s$, and $[x/u]T_2$ **indep** $s$, and $[x/u]T_3$ **indep** $s$. By (TX-Met) and (TI-Met).

□

**Lemma 5.26** (SubEq)**.** *If $\rho \vdash T_1 \approx T_2$, then $\rho \vdash [x/u]T_1 \approx [x/u]T_2$.*

*Proof.* Induction on $\rho \vdash T_1 \approx T_2$:

- Case (TE-Refl): $T_1 = T_2$, therefore $[x/u]T_1 = [x/u]T_2$. By (TE-Refl).
- Case (TE-And): $T_1 = T_3 \wedge T_4$, and $T_2 = T_5 \wedge T_6$, and $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$. By induction, $\rho \vdash [x/u]T_3 \approx [x/u]T_5$, and $\rho \vdash [x/u]T_4 \approx [x/u]T_6$. By (TE-And) and (TX-And).
- Case (TE-Or): $T_1 = T_3 \vee T_4$, and $T_2 = T_5 \vee T_6$, and $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$. By induction, $\rho \vdash [x/u]T_3 \approx [x/u]T_5$, and $\rho \vdash [x/u]T_4 \approx [x/u]T_6$. By (TE-Or) and (TX-Or).
- Case (TE-Sel): $T_1 = x_1.A(x_3)$, and $T_2 = x_2.A(x_3)$, and $\rho \vdash x_1 \approx x_2$. By 5.1(EqVKind), exist $v_1$, $v_2$, such that $x_1 = v_1$, and $x_2 = v_2$, therefore $x_1 \neq u$, and $x_2 \neq u$. By (VX-VarN), $[x/u]x_1 = x_1$, and $[x/u]x_2 = x_2$, therefore $\rho \vdash [x/u]x_1 \approx [x/u]x_2$. By (TE-Sel).
- Case (TE-Rec): $T_1 = \mu(s_1 : T_3)$, and $T_2 = \mu(s_1 : T_4)$, and $\rho \vdash T_3 \approx T_4$.

  Using alpha-equivalence, assume that $s_1 \neq u$, and $s_1 \neq x$. By induction, $\rho \vdash [x/u]T_3 \approx [x/u]T_4$. By (TE-Rec), $\rho \vdash \mu(s_1 : [x/u]T_3) \approx \mu(s_1 : [x/u]T_4)$. By (TX-Rec).
- Case (TE-Fld): $T_1 = \{a : T_3..T_4\}$, and $T_2 = \{a : T_5..T_6\}$, and $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$. By induction, $\rho \vdash [x/u]T_3 \approx [x/u]T_5$, and $\rho \vdash [x/u]T_4 \approx [x/u]T_6$. By (TE-Fld) and (TX-Fld).
- Case (TE-Typ): $T_1 = \{B(r) : T_3..T_4\}$, and $T_2 = \{B(r) : T_5..T_6\}$, and $\rho \vdash T_3 \approx T_5$, and $\rho \vdash T_4 \approx T_6$.

  Using alpha-equivalence, assume that $r \neq u$, and $r \neq x$. By induction, $\rho \vdash [x/u]T_3 \approx [x/u]T_5$, and $\rho \vdash [x/u]T_4 \approx [x/u]T_6$. By (TE-Typ) and (TX-Typ).
- Case (TE-Met): $T_1 = \{m(z : T_3, r : T_5) : T_4\}$, and $T_2 = \{m(z : T_6, r : T_8) : T_7\}$, and $\rho \vdash T_3 \approx T_6$, and $\rho \vdash T_4 \approx T_7$, and $\rho \vdash T_5 \approx T_8$.

  Using alpha-equivalence, assume that $r \neq u$, and $r \neq x$, and $z \neq u$, and $z \neq x$. By induction, $\rho \vdash [x/u]T_3 \approx [x/u]T_6$, and $\rho \vdash [x/u]T_4 \approx [x/u]T_7$, and $\rho \vdash [x/u]T_5 \approx [x/u]T_8$. By (TE-Met) and (TX-Met).

□

The following lemmata 5.27(SubV) and 5.28(SubT) are the main substitution lemmata for variable, term and definition typing, subtyping and splitting.

**Lemma 5.27** (SubV). *The following holds for variable typing, subtyping, splitting:*

- *If* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_1 : T_1$, *and* $u \notin \Gamma_1$ *and* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x : [x/u]T_2$, *then* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_1$.
- *If* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3 <: T_1$, *and* $u \notin \Gamma_1$ *and* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x : [x/u]T_2$, *then* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_1$.
- *If* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3$ $\mathbf{ro}$ $T_1$, *and* $u \notin \Gamma_1$ *and* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x : [x/u]T_2$, *then* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3$ $\mathbf{ro}$ $[x/u]T_1$.
- *If* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3$ $\mathbf{mu}(r_1)$ $T_4$, *and* $u \neq r_1$ *and* $x \neq r_1$, *and* $u \notin \Gamma_1$ *and* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x : [x/u]T_2$, *then* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3$ $\mathbf{mu}(r_1)$ $[x/u]T_4$.

*Proof idea.* Straightforward induction on typing of $x_1$, subtyping and splitting. (Adapted from kDOT [2], Lemma 4.6.3 (page 40).) ▽

*Proof.* Induction on typing, subtyping, splitting:

- Case (VT-Var): $\Gamma_1, u : T_2, \Gamma_2 = \Gamma_3, x_1 : T_1, \Gamma_4$, where $x_1 \notin \mathrm{dom}\, \Gamma_4$.
  - If $\Gamma_1 = \Gamma_3$. $x_1 = u$, and $T_1 = T_2$. By (VX-VarE), $[x/u]x_1 = x$. Trivially, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_1$.
  - If $\Gamma_1 = \Gamma_3, x_1 : T_1, \Gamma_5$. $\Gamma_4 = \Gamma_5, u : T_2, \Gamma_2$, therefore $x_1 \neq u$. By (VT-Var), $\Gamma_1, [x/u]\Gamma_2; \rho \vdash x_1 : T_1$. By (VX-VarE), $[x/u]x_1 = x_1$. By alpha-equivalence, we can assume that, $u \notin \mathrm{fv}\, \Gamma_1$, therefore $[x/u]T_1 = T_1$.
  - If $\Gamma_3 = \Gamma_1, u : T_2, \Gamma_5$. $\Gamma_2 = \Gamma_5, x_1 : T_1, \Gamma_4$. By (VT-Var), $\Gamma_1, [x/u]\Gamma_5, [x/u]x_1 : [x/u]T_1, [x/u]\Gamma_4; \rho \vdash [x/u]x_1 : [x/u]T_1$.
- Case (VT-RecE): $T_1 = [x_1/s]T_4$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_1 : \mu(s : T_4)$, and $T_4$ $\mathbf{indep}$ $s$. Using alpha-equivalence, assume that $s \neq u$, and $s \neq x$.

  By induction on variable typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : \mu(s : [x/u]T_4)$. By 5.25(SubIndep), $[x/u]T_4$ $\mathbf{indep}$ $s$. By (VT-RecE), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [[x/u]x_1/s][x/u]T_4$. By 5.21(SubSwap), $[[x/u]x_1/s][x/u]T_4 = [x/u]T_1$.
- Case (VT-RecI): $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_1 : [x_1/s]T_4$, and $T_1 = \mu(s : T_4)$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash [x_1/s]T_4$ $\mathbf{ro}$ $[x_1/s]T_4$, and $T_4$ $\mathbf{indep}$ $s$. Using alpha-equivalence, assume that $s \neq u$, and $s \neq x$.

  By induction on ro splitting, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u][x_1/s]T_4$ $\mathbf{ro}$ $[x/u][x_1/s]T_4$. By induction on variable typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u][x_1/s]T_4$. By 5.21(SubSwap), $[x/u][x_1/s]T_4 = [[x/u]x_1/s][x/u]T_4$. By 5.25(SubIndep), $[x/u]T_4$ $\mathbf{indep}$ $s$. By (VT-RecI), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : \mu(s : [x/u]T_4)$.
- Case (VT-AndI): $T_1 = T_4 \wedge T_5$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_1 : T_4$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_1 : T_5$. By induction on variable typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_4$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_5$. By (VT-AndI) and (TX-And), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_1$.
- Case (VT-MutTop): $T_1 = \{\mathsf{M}(r_0) : \bot..\top\}$. Directly by (VT-MutTop) and (TX-Top) and (TX-Bot) and (TX-Typ).
- Case (VT-Sub): $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_1 : T_4$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_4 <: T_1$. By induction on variable typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_4$. By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_4 <: [x/u]T_1$. By (VT-Sub), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_1$.
- Case (ST-Top): $T_1 = \top$. Directly by (ST-Top) and (TX-Top).
- Case (ST-Bot): $T_3 = \bot$. Directly by (ST-Bot) and (TX-Bot).
- Case (ST-Refl): $T_3 = T_1$. Directly by (ST-Refl).
- Case (ST-And1): $T_3 = T_1 \wedge T_4$. By (ST-And1), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_4 \wedge [x/u]T_1 <: [x/u]T_1$. By (TX-And).
- Case (ST-And2): $T_3 = T_4 \wedge T_1$. By (ST-And2), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_4 \wedge [x/u]T_1 <: [x/u]T_1$. By (TX-And).

- Case (ST-Or1): $T_1 = T_3 \vee T_4$. By (ST-Or1), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_3 \vee [x/u]T_4$. By (TX-Or).
- Case (ST-Or2): $T_1 = T_4 \vee T_3$. By (ST-Or2), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_4 \vee [x/u]T_3$. By (TX-Or).
- Cases (ST-N-M), (ST-N-Rec), (ST-N-Typ), (ST-N-Fld), (ST-N-Met): directly.
- Case (ST-And): $T_1 = T_4 \wedge T_5$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3 <: T_4$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3 <: T_5$. By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_4$, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_5$. By (ST-And), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_4 \wedge [x/u]T_5$. By (TX-And).
- Case (ST-Or): $T_3 = T_4 \vee T_5$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_4 <: T_1$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_5 <: T_1$. By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_4 <: [x/u]T_1$, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_5 <: [x/u]T_1$. By (ST-Or), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_4 \vee [x/u]T_5 <: [x/u]T_1$. By (TX-Or).
- Case (ST-Trans): $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3 <: T_4$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_4 <: T_1$.

  By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_4$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_4 <: [x/u]T_1$. By (ST-Trans), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_1$.
- Case (ST-SelU): $T_3 = x_3.B(x_2)$, and $T_1 = [x_2/r]T_5$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$.

  By induction on variable typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : [x/u]\{B(r) : T_4..T_5\}$. By (TX-Typ), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : \{B(r) : [x/u]T_4..[x/u]T_5\}$. By (ST-SelU), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3.B([x/u]x_2) <: [[x/u]x_2/r][x/u]T_5$. By 5.21(SubSwap) and (TX-Sel), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3.B(x_2) <: [x/u][x_2/r]T_5$.
- Case (ST-SelL): $T_3 = [x_2/r]T_4$, and $T_1 = x_3.B(x_2)$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$.

  Similarly as (ST-SelU). By induction on variable typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : [x/u]\{B(r) : T_4..T_5\}$. By (TX-Typ), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : \{B(r) : [x/u]T_4..[x/u]T_5\}$. By (ST-SelL), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [[x/u]x_2/r][x/u]T_4 <: [x/u]x_3.B([x/u]x_2)$. By 5.21(SubSwap) and (TX-Sel), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u][x_2/r]T_4 <: [x/u]x_3.B(x_2)$.
- Case (ST-Fld): $T_3 = \{a : T_4..T_5\}$, and $T_1 = \{a : T_6..T_7\}$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_6 <: T_4$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_5 <: T_7$.

  By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_6 <: [x/u]T_4$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_5 <: [x/u]T_7$. By (ST-Fld) and (TX-Fld).
- Case (ST-Typ): $T_3 = \{B(r) : T_4..T_5\}$, and $T_1 = \{B(r) : T_6..T_7\}$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_6 <: T_4$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_5 <: T_7$. Using alpha-equivalence, assume that $u$, $x$ are disjoint from $r$.

  By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_6 <: [x/u]T_4$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_5 <: [x/u]T_7$. By (ST-Typ) and (TX-Typ).
- Case (ST-Met): $T_3 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_7 <: T_4$, and $\Gamma_1, u : T_2, \Gamma_2, z : T_7;\rho \vdash T_9 <: T_6$, and $\Gamma_1, u : T_2, \Gamma_2, z : T_7, r : T_9;\rho \vdash T_5 <: T_8$. Using alpha-equivalence, assume that $u$, $x$ are disjoint from $z$ and $r$.

  By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_7 <: [x/u]T_4$. By induction on subtyping, $\Gamma_1, [x/u]\Gamma_2, z : [x/u]T_7;\rho \vdash [x/u]T_9 <: [x/u]T_6$, and $\Gamma_1, [x/u]\Gamma_2, z : [x/u]T_7, r : [x/u]T_9;\rho \vdash [x/u]T_5 <: [x/u]T_8$. By (ST-Met) and (TX-Met).
- Case (ST-Eq): $\rho \vdash T_3 \approx T_1$. By 5.26(SubEq), $\rho \vdash [x/u]T_3 \approx [x/u]T_1$.
- Case (ST-TypAnd): $T_3 = \{B(r) : T_4..T_5\} \wedge \{B(r) : T_6..T_7\}$, and $T_1 = \{B(r) : T_4 \vee T_6..T_5 \wedge T_7\}$. By (ST-TypAnd) and (TX-And) and (TX-Or) and (TX-Typ).
- Case (ST-Dist): $T_3 = T_4 \wedge (T_5 \vee T_6)$. $T_1 = (T_4 \wedge T_5) \vee (T_4 \wedge T_6)$. By (ST-Dist) and (TX-Or) and (TX-And).
- Case (TS-Top): $T_3 = \top$, and $T_1 = \top$, and $T_4 = \top$. By (TS-Top) and (TX-Top).
- Case (TS-Bot): $T_3 = \bot$, and $T_1 = \mathsf{N}$, and $T_4 = \bot$. By (TS-Bot) and (TX-Bot) and (TX-N).
- Case (TS-M): $T_3 = \{\mathsf{M}(r_1) : T_5..T_4\}$, and $T_1 = \top$. By (TS-M) and (TX-Typ).
- Case (TS-Typ): By (TS-Typ).
- Case (TS-Fld): By (TS-Fld).
- Case (TS-Met): By (TS-Met).
- Case (TS-Rec): By (TS-Rec).

- Case (TS-Sel): $T_3 = x_3.B(x_2)$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : \{B(r) : T_5..T_6\}$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash [x_2/r]T_6$ **ro** $T_1$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash [x_2/r]T_6\ \mathbf{mu}(r_1)\ T_4$.

  By induction on variable typing and splitting, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : [x/u]\{B(r) : T_5..T_6\}$, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u][x_2/r]T_6$ **ro** $[x/u]T_1$, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u][x_2/r]T_6\ \mathbf{mu}(r_1)\ [x/u]T_4$. By (TX-Typ), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : \{B(r) : [x/u]T_5..[x/u]T_6\}$. By 5.21(SubSwap), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [[x/u]x_2/r][x/u]T_6$ **ro** $[x/u]T_1$, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [[x/u]x_2/r][x/u]T_6\ \mathbf{mu}(r_1)\ [x/u]T_4$. By (TS-Sel), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3.B([x/u]x_2)$ **ro** $[x/u]T_1$, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3.B([x/u]x_2)\ \mathbf{mu}(r_1)\ [x/u]T_4$. By (TX-Sel).

- Case (TS-AndR): $T_3 = T_5 \wedge T_6$, and $T_1 = T_7 \wedge T_8$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_5$ **ro** $T_7$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_6$ **ro** $T_8$.

  By induction on splitting, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_5$ **ro** $[x/u]T_7$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_6$ **ro** $[x/u]T_8$. By (TS-AndR) and (TX-And).

- Case (TS-AndM): $T_3 = T_5 \wedge T_6$, and $T_4 = T_7 \wedge T_8$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_5\ \mathbf{mu}(r_1)\ T_7$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_6\ \mathbf{mu}(r_1)\ T_8$.

  By induction on splitting, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_5\ \mathbf{mu}(r_1)\ [x/u]T_7$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_6\ \mathbf{mu}(r_1)\ [x/u]T_8$. By (TS-AndM) and (TX-And).

- Case (TS-OrR): $T_3 = T_5 \vee T_6$, and $T_1 = T_7 \vee T_8$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_5$ **ro** $T_7$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_6$ **ro** $T_8$.

  By induction on splitting, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_5$ **ro** $[x/u]T_7$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_6$ **ro** $[x/u]T_8$. By (TS-OrR) and (TX-Or).

- Case (TS-OrM): $T_3 = T_5 \vee T_6$, and $T_4 = T_7 \vee T_8$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_5\ \mathbf{mu}(r_1)\ T_7$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_6\ \mathbf{mu}(r_1)\ T_8$.

  By induction on splitting, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_5\ \mathbf{mu}(r_1)\ [x/u]T_7$, and $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_6\ \mathbf{mu}(r_1)\ [x/u]T_8$. By (TS-OrM) and (TX-Or).

□

**Lemma 5.28** (SubT)**.** *The following holds for term and definition typing:*

- *If* $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash t : T_1$, *and* $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x$, *and* $u \notin \Gamma_1$ *and* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x : [x/u]T_2$, *then* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [x/u]T_1$.

- *If* $\Gamma_1, u : T_2, \Gamma_2, s : T_3;\rho \vdash d : T_1$, *and* $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x$ *and* $u \neq s$ *and* $x \neq s$, *and* $u \notin \Gamma_1$ *and* $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x : [x/u]T_2$, *then* $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash [x/u]d : [x/u]T_1$.

*Idea.* Substitution preserves typing of terms and definitions. ▽

*Proof idea.* (Adapted from kDOT [2], Lemma 4.6.3 (page 40).) Induction on term typing and definition typing, using 5.27(SubV). ▽

*Proof.* Induction on $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash t : T_1$:

- Case (TT-Var): $t = \text{v}x_1$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_1 : T_1$, and $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x_1$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_1 : [x/u]T_1$. By 5.24(SubVis), $\Gamma_1, [x/u]\Gamma_2$ **vis** $[x/u]x_1$. By (TT-Var) and (EX-Var), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]\text{v}x_1 : [x/u]T_1$.

- Case (TT-Apply): $t = x_3.m\,x_2$. $T_1 = [x_3/r][x_2/z]T_4$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : \{m(z : T_3, r : T_5) : T_4\}$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_2 : T_3$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : [x_2/z]T_5$. $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x_3$. $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x_2$.

  Using alpha-equivalence, assume that $u$, $x$, $x_3$ and $x_2$ are disjoint from $z$ and $r$.

  By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : [x/u]\{m(z : T_3, r : T_5) : T_4\}$. By (TX-Met), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : \{m(z : [x/u]T_3, r : [x/u]T_5) : [x/u]T_4\}$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_2 : [x/u]T_3$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]x_3 : [x/u][x_2/z]T_5$. By 5.21(SubSwap), $\Gamma;\rho \vdash [x/u]x_3 : [x_2/z][x/u]T_5$. By 5.24(SubVis), $\Gamma_1, [x/u]\Gamma_2$ **vis** $[x/u]x_3$, and $\Gamma_1, [x/u]\Gamma_2$ **vis** $[x/u]x_2$. By (TT-Apply) and (EX-Apply), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [[x/u]x_3/r][[x/u]x_2/z][x/u]T_4$. By 5.21(SubSwap), $[x/u]T_1 = [x/u][x_3/r][x_2/z]T_4 = [[x/u]x_3/r][x/u][x_2/z]T_4 = [[x/u]x_3/r][[x/u]x_2/z][x/u]T_4$.

- Case (TT-Read): $t = x_3.a$. $T_1 = T_5 \wedge \{\mathsf{M}(r_0) : \bot..(T_6 \vee x_3.\mathsf{M}(r_0))\}$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : \{a : T_3..T_4\}$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_4$ **ro** $T_5$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_4$ $\mathbf{mu}(r_0)$ $T_6$. $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x_3$.

  By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x_3 : [x/u]\{a : T_3..T_4\}$. By (TX-Fld), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x_3 : \{a : [x/u]T_3..[x/u]T_4\}$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash T_4$ **ro** $[x/u]T_5$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash T_4$ $\mathbf{mu}(r_0)$ $[x/u]T_6$. By 5.24(SubVis), $\Gamma_1, [x/u]\Gamma_2$ **vis** $[x/u]x_3$. By (TT-Read) and (EX-Read), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [x/u]T_5 \wedge \{\mathsf{M}(r_0) : \bot..([x/u]T_6 \vee [x/u]x_3.\mathsf{M}(r_0))\}$. By (TX-Sel) and (TX-Or) and (TX-Typ) and (TX-And), $[x/u]T_1 = [x/u]T_5 \wedge \{\mathsf{M}(r_0) : \bot..(T_6 \vee x_3.\mathsf{M}(r_0))\} = [x/u]T_5 \wedge \{\mathsf{M}(r_0) : \bot..([x/u]T_6 \vee [x/u]x_3.\mathsf{M}(r_0))\}$.

- Case (TT-Write): $t = x_3.a := x_2$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_2 : T_3$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : \{a : T_3..T_1\}$. $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash x_3 : \{\mathsf{M}(r_0) : \bot..\bot\}$. $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x_3$. $\Gamma_1, u : T_2, \Gamma_2$ **vis** $x_2$.

  By 5.24(SubVis), $\Gamma_1, [x/u]\Gamma_2$ **vis** $[x/u]x_3$, and $\Gamma_1, [x/u]\Gamma_2$ **vis** $[x/u]x_2$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x_2 : [x/u]T_3$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x_3 : [x/u]\{a : T_3..T_1\}$. By (TX-Fld), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x_3 : \{a : [x/u]T_3..[x/u]T_1\}$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x_3 : [x/u]\{\mathsf{M}(r_0) : \bot..\bot\}$. By (TX-Typ) and (TX-Bot), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash x_3 : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (TT-Write) and (EX-Write), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [x/u]T_1$.

- Case (TT-New): $t = \mathsf{let}\ z = \nu(s : T_3)d\ \mathsf{in}\ t_1$. $\Gamma_1, u : T_2, \Gamma_2, s : T_3;\rho \vdash d : T_3$. $\Gamma_1, u : T_2, \Gamma_2, z : \mu(s : T_3) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash t_1 : T_1$. $z \notin \text{fv}\ T_1$. $T_3$ **indep** $s$.

  Using alpha-equivalence, assume that $u$ and $x$ are disjoint from $z$ and $s$.

  By induction on definition typing, $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash [x/u]d : [x/u]T_3$. By induction on term typing, $\Gamma_1, [x/u]\Gamma_2, z : [x/u]\mu(s : T_3) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash [x/u]t_1 : [x/u]T_1$. By (TX-Typ) and (TX-Bot), $\Gamma_1, [x/u]\Gamma_2, z : \mu(s : [x/u]T_3) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash [x/u]t_1 : [x/u]T_1$. Because $x \neq z$, therefore $z \notin \text{fv}\ [x/u]T_1$. By 5.25(SubIndep). $[x/u]T_3$ **indep** $s$. By (TT-New) and (EX-LetNew), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [x/u]T_1$.

- Case (TT-Let): $t = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$, where $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash t_1 : T_3$, and $\Gamma_1, u : T_2, \Gamma_2, z : T_3;\rho \vdash t_2 : T_1$, and $z \notin \text{fv}\ T_1$.

  Using alpha-equivalence, assume that $u$ and $x$ are disjoint from $z$.

  By induction on term typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t_1 : [x/u]T_3$. By induction on term typing, $\Gamma_1, [x/u]\Gamma_2, z : [x/u]T_3;\rho \vdash [x/u]t_2 : [x/u]T_1$. Because $x \neq z$, therefore $z \notin \text{fv}\ [x/u]T_1$. By (TT-Let) and (EX-Let), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [x/u]T_1$.

- Case (TT-Sub): $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash t : T_3$, and $\Gamma_1, u : T_2, \Gamma_2;\rho \vdash T_3 <: T_1$. By induction on term typing, $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [x/u]T_3$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]T_3 <: [x/u]T_1$. By (TT-Sub), $\Gamma_1, [x/u]\Gamma_2;\rho \vdash [x/u]t : [x/u]T_1$.

- Case (DT-Typ): $d = \{A(r) = T_4\}$, and $T_1 = \{A(r) : T_4..T_4\}$. Using alpha-equivalence, assume that $u$ and $x$ are disjoint from $r$.

  By (DT-Typ), $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash \{A(r) = [x/u]T_4\} : \{A(r) : [x/u]T_4..[x/u]T_4\}$. By (DX-Typ) and (TX-Typ).

- Case (DT-TypB): $d = \{A(r) = T_4\}$, and $T_1 = \{A(r) : \bot..T_4\}$. Using alpha-equivalence, assume that $u$ and $x$ are disjoint from $r$.

  By (DT-TypB), $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash \{A(r) = [x/u]T_4\} : \{A(r) : \bot..[x/u]T_4\}$. By (DX-Typ) and (TX-Bot) and (TX-Typ).

- Case (DT-Fld): $d = \{a = x_3\}$, and $T_1 = \{a : T_4..T_4\}$, where $\Gamma_1, u : T_2, \Gamma_2, s : T_3$ **vis** $x_3$, and $\Gamma_1, u : T_2, \Gamma_2, s : T_3;\rho \vdash x_3 : T_4$.

  By 5.24(SubVis), $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3$ **vis** $[x/u]x_3$. By 5.27(SubV), $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash [x/u]x_3 : [x/u]T_4$. By (DT-Fld), $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash \{a = [x/u]x_3\} : \{a : [x/u]T_4..[x/u]T_4\}$. By (DX-Fld) and (TX-Fld).

- Case (DT-Met): $d = \{m(z, r) = t\}$, and $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, where $\Gamma_1, u : T_2, \Gamma_2, s : T_3, !, z : T_4, r : T_3 \wedge [r/s]T_3 \wedge T_6;\rho \vdash t : T_5$, and $z \notin \text{fv}\ T_4 \cup \text{fv}\ T_3$, and $r \notin \text{fv}\ T_4 \cup \text{fv}\ T_6 \cup \text{fv}\ T_3$. Using alpha-equivalence, assume that $u$ and $x$ are disjoint from $r$ and $z$.

  By induction, $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3, !, z : [x/u]T_4, r : [x/u]T_3 \wedge [r/s][x/u]T_3 \wedge [x/u]T_6;\rho \vdash [x/u]t : [x/u]T_5$. By (DT-Met), $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash \{m(z, r) = [x/u]t\} : \{m(z : [x/u]T_4, r : [x/u]T_6) : [x/u]T_5\}$. By (DX-Met) and (TX-Met).

- Case (DT-And): $d = d_1 \wedge d_2$, and $T_1 = T_4 \wedge T_5$, where $\Gamma_1, u : T_2, \Gamma_2, s : T_3;\rho \vdash d_1 : T_4$, and $\Gamma_1, u : T_2, \Gamma_2, s : T_3;\rho \vdash d_2 : T_5$, and $d_1$ and $d_2$ have distinct member names.

  By induction on definition typing, $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash [x/u]d_1 : [x/u]T_4$, and $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash [x/u]d_2 : [x/u]T_5$. By (DT-And), $\Gamma_1, [x/u]\Gamma_2, s : [x/u]T_3;\rho \vdash [x/u]d_1 \wedge [x/u]d_2 : [x/u]T_4 \wedge [x/u]T_5$. By (DX-And) and (TX-And).

□

The lemma 5.29(SubD) relates definition typing and heap item typing. While the definitions appear in terms, where during execution, fields are assigned reference variables, on the heap fields contain locations. Definitions can also refer to the self variable $s$ of the object, which on heap is replaced by the actual location of the object. This lemma shows that replacing the $s$ self variable by the object location, given definition typing, gives us heap item typing.

**Lemma 5.29** (SubD). *If* $\Gamma, s : T_3;\rho \vdash d : T_1$, *and* $s \notin \Gamma$ *and* $\Gamma$ **vis** $y$ *and* $\Gamma;\rho \vdash y : [y/s]T_3$, *then* $\Gamma, y/s : T_3;\rho \vdash [y/s]d : [y/s]T_1$.

*Idea.* Substitution of self variable preserves definition typing. ▽

*Proof idea.* Induction on definition typing. ▽

*Proof.* Induction on definition typing:

- Case (DT-Typ): $d = \{A(r) = T_4\}$, and $T_1 = \{A(r) : T_4..T_4\}$.

  By (HT-Typ), $\Gamma, y/s : T_3;\rho \vdash \{A(r) = [y/s]T_4\} : \{A(r) : [y/s]T_4..[y/s]T_4\}$. By (DX-Typ) and (TX-Typ).

- Case (DT-TypB): $d = \{A(r) = T_4\}$, and $T_1 = \{A(r) : \bot..T_4\}$.

  By (HT-TypB), $\Gamma, y/s : T_3;\rho \vdash \{A(r) = [y/s]T_4\} : \{A(r) : \bot..[y/s]T_4\}$. By (DX-Typ) and (TX-Bot) and (TX-Typ).

- Case (DT-Fld): $d = \{a = x_3\}$, and $T_1 = \{a : T_4..T_4\}$, where $\Gamma, s : T_3$ **vis** $x_3$, and $\Gamma, s : T_3;\rho \vdash x_3 : T_4$.

  By 5.24(SubVis), $\Gamma$ **vis** $[y/s]x_3$. By 5.27(SubV), $\Gamma;\rho \vdash [y/s]x_3 : [y/s]T_4$. By (HT-Fld), $\Gamma, y/s : T_3;\rho \vdash \{a = [y/s]x_3\} : \{a : [y/s]T_4..[y/s]T_4\}$. By (DX-Fld) and (TX-Fld).

- Case (DT-Met): $d = \{m(z, r) = t\}$, and $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, where $\Gamma, s : T_3, !, z : T_4, r : T_3 \wedge [r/s]T_3 \wedge T_6;\rho \vdash t : T_5$, and $z \notin \text{fv } T_4 \cup \text{fv } T_3$, and $r \notin \text{fv } T_4 \cup \text{fv } T_6 \cup \text{fv } T_3$.

  By 5.28(SubT) and (TX-And), $\Gamma, !, z : [y/s]T_4, r : [y/s]T_3 \wedge [y/s][r/s]T_3 \wedge [y/s]T_6;\rho \vdash [y/s]t : [y/s]T_5$. By 5.23(SubId), $[y/s][r/s]T_3 = [r/s]T_3$, therefore $\Gamma, !, z : [y/s]T_4, r : [y/s]T_3 \wedge [r/s]T_3 \wedge [y/s]T_6;\rho \vdash [y/s]t : [y/s]T_5$. By (HT-Met), $\Gamma, y/s : T_3;\rho \vdash \{m(z, r) = [y/s]t\} : \{m(z : [y/s]T_4, r : [y/s]T_6) : [y/s]T_5\}$. By (DX-Met) and (TX-Met).

- Case (DT-And): $d = d_1 \wedge d_2$, and $T_1 = T_4 \wedge T_5$, where $\Gamma, s : T_3;\rho \vdash d_1 : T_4$, and $\Gamma, s : T_3;\rho \vdash d_2 : T_5$, and $d_1$ and $d_2$ have distinct member names.

  By induction on definition typing, $\Gamma, y/s : T_3;\rho \vdash [y/s]d_1 : [y/s]T_4$, and $\Gamma, y/s : T_3;\rho \vdash [y/s]d_2 : [y/s]T_5$. By (HT-And), $\Gamma, y/s : T_3;\rho \vdash [y/s]d_1 \wedge [y/s]d_2 : [y/s]T_4 \wedge [y/s]T_5$. By (DX-And) and (TX-And).

□

The runtime environment $\rho$ relates references to heap locations. A reference to the same object as a location has the same type except mutability. The location is always mutable, so it is safe to replace the reference by the corresponding location.

First, the lemmata 5.30(SubEqEV) and 5.31(SubEqET) show that replacing a reference by the location preserves equivalence. Then the lemma 5.32(SubW) shows that it preserves typing, subtyping and splitting.

**Lemma 5.30** (SubEqEV). *If* $\rho_1, w \to y, \rho_2 \vdash v_1 \approx v_2$, *then* $\rho_1, \rho_2 \vdash [y/w]v_1 \approx [y/w]v_2$.

*Proof.* Induction on $\rho_1, w \to y, \rho_2 \vdash v_1 \approx v_2$:

- Case (VE-RtoL): $v_1 \to v_2 \in \rho_1, w \to y, \rho_2$.
  - If $v_2 = w$. Not possible because $w \notin \rho_1$, and $w \notin \rho_2$.

  - If $v_1 = w$, and $v_2 \neq w$, then because $w \notin \rho_1$, and $w \notin \rho_2$, we have $v_2 = y$, then by (VX-VarE) and (VX-VarN), $[y/w]v_1 = y$, and $[y/w]v_2 = y$. By (VE-Refl).
  - If $v_1 \neq w$, and $v_2 \neq w$, then by (VX-VarN), $[y/w]v_1 = v_1$, and $[y/w]v_2 = v_2$. Trivially.

- Case (VE-Refl): $v_1 = v_2$, therefore $[y/w]v_1 = [y/w]v_2$. By (VE-Refl).
- Case (VE-Symm): $\rho_1, w \to y, \rho_2 \vdash v_2 \approx v_1$. By induction, $\rho_1, \rho_2 \vdash [y/w]v_2 \approx [y/w]v_1$. By (VE-Symm).
- Case (VE-Trans): $\rho_1, w \to y, \rho_2 \vdash v_1 \approx v_3$, and $\rho_1, w \to y, \rho_2 \vdash v_3 \approx v_2$. By induction, $\rho_1, \rho_2 \vdash [y/w]v_1 \approx [y/w]v_3$, and $\rho_1, \rho_2 \vdash [y/w]v_3 \approx [y/w]v_2$. By (VE-Trans).

□

**Lemma 5.31** (SubEqET). *If $\rho_1, w \to y, \rho_2 \vdash T_1 \approx T_2$, then $\rho_1, \rho_2 \vdash [y/w]T_1 \approx [y/w]T_2$.*

*Proof.* Induction on $\rho_1, w \to y, \rho_2 \vdash T_1 \approx T_2$:

- Case (TE-Refl): $T_1 = T_2$, therefore $[y/w]T_1 = [y/w]T_2$. By (TE-Refl).
- Case (TE-And): $T_1 = T_3 \wedge T_4$, and $T_2 = T_5 \wedge T_6$, and $\rho_1, w \to y, \rho_2 \vdash T_3 \approx T_5$, and $\rho_1, w \to y, \rho_2 \vdash T_4 \approx T_6$. By induction, $\rho_1, \rho_2 \vdash [y/w]T_3 \approx [y/w]T_5$, and $\rho_1, \rho_2 \vdash [y/w]T_4 \approx [y/w]T_6$. By (TE-And) and (TX-And).
- Case (TE-Or): $T_1 = T_3 \vee T_4$, and $T_2 = T_5 \vee T_6$, and $\rho_1, w \to y, \rho_2 \vdash T_3 \approx T_5$, and $\rho_1, w \to y, \rho_2 \vdash T_4 \approx T_6$. By induction, $\rho_1, \rho_2 \vdash [y/w]T_3 \approx [y/w]T_5$, and $\rho_1, \rho_2 \vdash [y/w]T_4 \approx [y/w]T_6$. By (TE-Or) and (TX-Or).
- Case (TE-Sel): $T_1 = x_1.A(x_3)$, and $T_2 = x_2.A(x_3)$, and $\rho_1, w \to y, \rho_2 \vdash x_1 \approx x_2$. By 5.1(EqVKind), exist $v_1$, $v_2$, such that $x_1 = v_1$, and $x_2 = v_2$. By 5.30(SubEqEV), $\rho_1, \rho_2 \vdash [y/w]x_1 \approx [y/w]x_2$. By (TE-Sel).
- Case (TE-Rec): $T_1 = \mu(s_1 : T_3)$, and $T_2 = \mu(s_1 : T_4)$, and $\rho_1, w \to y, \rho_2 \vdash T_3 \approx T_4$.

  We know that $s_1 \neq w$, and $s_1 \neq y$. By induction, $\rho_1, \rho_2 \vdash [y/w]T_3 \approx [y/w]T_4$. By (TE-Rec), $\rho \vdash \mu(s_1 : [y/w]T_3) \approx \mu(s_1 : [y/w]T_4)$. By (TX-Rec).
- Case (TE-Fld): $T_1 = \{a : T_3..T_4\}$, and $T_2 = \{a : T_5..T_6\}$, and $\rho_1, w \to y, \rho_2 \vdash T_3 \approx T_5$, and $\rho_1, w \to y, \rho_2 \vdash T_4 \approx T_6$. By induction, $\rho_1, \rho_2 \vdash [y/w]T_3 \approx [y/w]T_5$, and $\rho_1, \rho_2 \vdash [y/w]T_4 \approx [y/w]T_6$. By (TE-Fld) and (TX-Fld).
- Case (TE-Typ): $T_1 = \{B(r) : T_3..T_4\}$, and $T_2 = \{B(r) : T_5..T_6\}$, and $\rho_1, w \to y, \rho_2 \vdash T_3 \approx T_5$, and $\rho_1, w \to y, \rho_2 \vdash T_4 \approx T_6$.

  We know that $r \neq w$, and $r \neq y$. By induction, $\rho \vdash [y/w]T_3 \approx [y/w]T_5$, and $\rho \vdash [y/w]T_4 \approx [y/w]T_6$. By (TE-Typ) and (TX-Typ).
- Case (TE-Met): $T_1 = \{m(z : T_3, r : T_5) : T_4\}$, and $T_2 = \{m(z : T_6, r : T_8) : T_7\}$, and $\rho_1, w \to y, \rho_2 \vdash T_3 \approx T_6$, and $\rho_1, w \to y, \rho_2 \vdash T_4 \approx T_7$, and $\rho_1, w \to y, \rho_2 \vdash T_5 \approx T_8$.

  We know that $r \neq w$, and $r \neq y$, and $z \neq w$, and $z \neq y$. By induction, $\rho_1, \rho_2 \vdash [y/w]T_3 \approx [y/w]T_6$, and $\rho_1, \rho_2 \vdash [y/w]T_4 \approx [y/w]T_7$, and $\rho_1, \rho_2 \vdash [y/w]T_5 \approx [y/w]T_8$. By (TE-Met) and (TX-Met).

□

**Lemma 5.32** (SubW). *The following holds for variable typing, subtyping, splitting :*

- *If $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_1 : T_1$, and $\Gamma_1, w : T_2, \Gamma_2 \sim \rho_1, w \to y, \rho_2$ and $w \notin \Gamma_1$ and $w \notin \rho_1$ and $w \notin \rho_2$, then $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [y/w]T_1$.*
- *If $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_3 <: T_1$, and $\Gamma_1, w : T_2, \Gamma_2 \sim \rho_1, w \to y, \rho_2$ and $w \notin \Gamma_1$ and $w \notin \rho_1$ and $w \notin \rho_2$, then $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_1$.*
- *If $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_3$ **ro** $T_1$, and $\Gamma_1, w : T_2, \Gamma_2 \sim \rho_1, w \to y, \rho_2$ and $w \notin \Gamma_1$ and $w \notin \rho_1$ and $w \notin \rho_2$, then $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3$ **ro** $[y/w]T_1$.*
- *If $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_3$ **mu**$(r_1)$ $T_4$, and $\Gamma_1, w : T_2, \Gamma_2 \sim \rho_1, w \to y, \rho_2$ and $w \notin \Gamma_1$ and $w \notin \rho_1$ and $w \notin \rho_2$, then $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3$ **mu**$(r_1)$ $[y/w]T_4$.*

*Proof.* Induction on variable typing, subtyping, splitting:

- Case (VT-Var): $\Gamma_1, w : T_2, \Gamma_2 = \Gamma_3, x_1 : T_1, \Gamma_4$, where $x_1 \notin \text{dom}\ \Gamma_4$.
  - If $\Gamma_1 = \Gamma_3$, then $x_1 = w$, and $T_1 = T_2$. By (VX-VarE), $[y/w]x_1 = y$. By 5.16(ECorrInvY), exists $T_4$, such that $\Gamma_1 = \Gamma_5, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_6$, and $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_4\}$. By (ST-Bot) and (ST-Typ) and (ST-Refl) and 5.18(AndSub), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: T_1$. By (VT-Var) and (VT-Sub), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash y : T_1$.
  - If $\Gamma_1 = \Gamma_3, x_1 : T_1, \Gamma_5$, therefore $x_1 \neq w$. By (VT-Var), $\Gamma_1, [y/w]\Gamma_2;\rho \vdash x_1 : T_1$. By (VX-VarE), $[y/w]x_1 = x_1$. By alpha-equivalence, we can assume that, $w \notin \text{fv}\ \Gamma_1$, therefore $[y/w]T_1 = T_1$.
  - If $\Gamma_3 = \Gamma_1, w : T_2, \Gamma_5$. $\Gamma_2 = \Gamma_5, x_1 : T_1, \Gamma_4$. By (VT-Var), $\Gamma_1, [y/w]\Gamma_5, [y/w]x_1 : [y/w]T_1, [y/w]\Gamma_4; \rho \vdash [y/w]x_1 : [y/w]T_1$.

- Case (VT-RecE): $T_1 = [x_1/s]T_4$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_1 : \mu(s : T_4)$, and $T_4$ **indep** $s$.

  By induction on variable typing, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : \mu(s : [y/w]T_4)$. By 5.25(SubIndep), $[y/w]T_4$ **indep** $s$. By (VT-RecE), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [[y/w]x_1/s][y/w]T_4$. By 5.21(SubSwap), $[[y/w]x_1/s][y/w]T_4 = [y/w]T_1$.

- Case (VT-RecI): $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_1 : [x_1/s]T_4$, and $T_1 = \mu(s : T_4)$, and $\Gamma_1, w : T_2, \Gamma_2; \rho_1, w \to y, \rho_2 \vdash [x_1/s]T_4$ **ro** $[x_1/s]T_4$, and $T_4$ **indep** $s$.

  By induction on ro splitting, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w][x_1/s]T_4$ **ro** $[y/w][x_1/s]T_4$. By induction on variable typing, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [y/w][x_1/s]T_4$. By 5.21(SubSwap), $[y/w][x_1/s]T_4 = [[y/w]x_1/s][y/w]T_4$. By 5.25(SubIndep), $[y/w]T_4$ **indep** $s$. By (VT-RecI), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : \mu(s : [y/w]T_4)$.

- Case (VT-AndI): $T_1 = T_4 \wedge T_5$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_1 : T_4$, and $\Gamma_1, w : T_2, \Gamma_2; \rho_1, w \to y, \rho_2 \vdash x_1 : T_5$. By induction on variable typing, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [y/w]T_4$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [y/w]T_5$. By (VT-AndI) and (TX-And), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [y/w]T_1$.
- Case (VT-MutTop): $T_1 = \{\mathsf{M}(r_0) : \bot..\top\}$. Directly by (VT-MutTop) and (TX-Top) and (TX-Bot) and (TX-Typ).
- Case (VT-Sub): $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_1 : T_4$. $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_4 <: T_1$. By induction on variable typing, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [y/w]T_4$. By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_4 <: [y/w]T_1$. By (VT-Sub), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_1 : [y/w]T_1$.
- Case (ST-Top): $T_1 = \top$. Directly by (ST-Top) and (TX-Top).
- Case (ST-Bot): $T_3 = \bot$. Directly by (ST-Bot) and (TX-Bot).
- Case (ST-Refl): $T_3 = T_1$. Directly by (ST-Refl).
- Case (ST-And1): $T_3 = T_1 \wedge T_4$. By (ST-And1), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_4 \wedge [y/w]T_1 <: [y/w]T_1$. By (TX-And).
- Case (ST-And2): $T_3 = T_4 \wedge T_1$. By (ST-And2), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_4 \wedge [y/w]T_1 <: [y/w]T_1$. By (TX-And).
- Case (ST-And): $T_1 = T_4 \wedge T_5$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_3 <: T_4$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_3 <: T_5$. By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_4$, $\Gamma_1, [y/w]\Gamma_2; \rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_5$. By (ST-And), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_4 \wedge [y/w]T_5$. By (TX-And).
- Case (ST-Or1): $T_1 = T_3 \vee T_4$. By (ST-Or1), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_3 \vee [y/w]T_4$. By (TX-Or).
- Case (ST-Or2): $T_1 = T_4 \vee T_3$. By (ST-Or2), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_4 \vee [y/w]T_3$. By (TX-Or).
- Case (ST-Or): $T_3 = T_4 \vee T_5$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_4 <: T_1$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_5 <: T_1$. By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_4 <: [y/w]T_1$, $\Gamma_1, [y/w]\Gamma_2; \rho_1, \rho_2 \vdash [y/w]T_5 <: [y/w]T_1$. By (ST-Or), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_4 \vee [y/w]T_5 <: [y/w]T_1$. By (TX-Or).
- Case (ST-Trans): $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_3 <: T_4$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_4 <: T_1$.

  By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_4$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_4 <: [y/w]T_1$. By (ST-Trans), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_3 <: [y/w]T_1$.

- Case (ST-SelL): $T_3 = [x_2/r]T_4$, and $T_1 = x_3.B(x_2)$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_3 : \{B(r) : T_4..T_5\}$.

  Similarly as (ST-SelU). By induction on variable typing, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3 : [y/w]\{B(r) : T_4..T_5\}$. By (TX-Typ), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3 : \{B(r) : [y/w]T_4..[y/w]T_5\}$. By (ST-SelL), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [[y/w]x_2/r][y/w]T_4 <: [y/w]x_3.B([y/w]x_2)$. By 5.21(SubSwap) and (TX-Sel), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w][x_2/r]T_4 <: [y/w]x_3.B(x_2)$.
- Case (ST-SelU): $T_3 = x_3.B(x_2)$, and $T_1 = [x_2/r]T_5$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_3 : \{B(r) : T_4..T_5\}$.

  By induction on variable typing, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3 : [y/w]\{B(r) : T_4..T_5\}$. By (TX-Typ), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3 : \{B(r) : [y/w]T_4..[y/w]T_5\}$. By (ST-SelU), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3.B([y/w]x_2) <: [[y/w]x_2/r][y/w]T_5$. By 5.21(SubSwap) and (TX-Sel), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3.B(x_2) <: [y/w][x_2/r]T_5$.
- Case (ST-Typ): $T_3 = \{B(r) : T_4..T_5\}$, and $T_1 = \{B(r) : T_6..T_7\}$, where $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_6 <: T_4$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_5 <: T_7$.

  By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_6 <: [y/w]T_4$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_5 <: [y/w]T_7$. By (ST-Typ) and (TX-Typ).
- Case (ST-Fld): $T_3 = \{a : T_4..T_5\}$, and $T_1 = \{a : T_6..T_7\}$, where $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_6 <: T_4$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_5 <: T_7$.

  By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_6 <: [y/w]T_4$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_5 <: [y/w]T_7$. By (ST-Fld) and (TX-Fld).
- Case (ST-Met): $T_3 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, where $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_7 <: T_4$, and $\Gamma_1, w : T_2, \Gamma_2, z : T_7;\rho_1, w \to y, \rho_2 \vdash T_9 <: T_6$, and $\Gamma_1, w : T_2, \Gamma_2, z : T_7, r : T_9;\rho_1, w \to y, \rho_2 \vdash T_5 <: T_8$.

  By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_7 <: [y/w]T_4$. By induction on subtyping, $\Gamma_1, [y/w]\Gamma_2, z : [y/w]T_7;\rho_1, \rho_2 \vdash [y/w]T_9 <: [y/w]T_6$, and $\Gamma_1, [y/w]\Gamma_2, z : [y/w]T_7, r : [y/w]T_9;\rho_1, \rho_2 \vdash [y/w]T_5 <: [y/w]T_8$. By (ST-Met) and (TX-Met).
- Case (ST-TypAnd): $T_3 = \{B(r) : T_4..T_5\} \wedge \{B(r) : T_6..T_7\}$, and $T_1 = \{B(r) : T_4 \vee T_6..T_5 \wedge T_7\}$. By (ST-TypAnd) and (TX-And) and (TX-Or) and (TX-Typ).
- Case (ST-Eq): $\rho_1, w \to y, \rho_2 \vdash T_3 \approx T_1$. By 5.31(SubEqET), $\rho_1, \rho_2 \vdash [y/w]T_3 \approx [y/w]T_1$. By (ST-Eq), $\rho_1, \rho_2;\Gamma_1, [y/w]\Gamma_2 \vdash [y/w]T_3 <: [y/w]T_1$.
- Case (ST-N-M): $T_3 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_1 = \bot$. By (ST-N-M) and (TX-Bot) and (TX-Typ) and (TX-N) and (TX-And).
- Case (ST-N-Rec): $T_3 = \mathsf{N}$, and $T_1 = \mu(s : T_4)$. By (ST-N-Rec) and (TX-Rec) and (TX-N).
- Case (ST-N-Fld): $T_3 = \mathsf{N}$, and $T_1 = \{a : T_6..T_7\}$. By (ST-N-Fld) and (TX-Fld) and (TX-N).
- Case (ST-N-Met): $T_3 = \mathsf{N}$, and $T_1 = \{m(z : T_7, r : T_9) : T_8\}$. By (ST-N-Met) and (TX-Met) and (TX-N).
- Case (ST-N-Typ): $T_3 = \mathsf{N}$, and $T_1 = \{B(r) : T_6..T_7\}$. By (ST-N-Typ) and (TX-Typ) and (TX-N).
- Case (ST-Dist): $T_3 = T_4 \wedge (T_5 \vee T_6)$. $T_1 = (T_4 \wedge T_5) \vee (T_4 \wedge T_6)$. By (ST-Dist) and (TX-Or) and (TX-And).
- Case (TS-Top): $T_3 = \top$, and $T_1 = \top$, and $T_4 = \top$. By (TS-Top) and (TX-Top).
- Case (TS-Bot): $T_3 = \bot$, and $T_1 = \mathsf{N}$, and $T_4 = \bot$. By (TS-Bot) and (TX-Bot) and (TX-N).
- Case (TS-M): $T_3 = \{\mathsf{M}(r_1) : T_5..T_4\}$, and $T_1 = \top$. By (TS-M) and (TX-Typ).
- Case (TS-Typ): By (TS-Typ).
- Case (TS-Fld): By (TS-Fld).
- Case (TS-Met): By (TS-Met).
- Case (TS-Rec): By (TS-Rec).
- Case (TS-Sel): $T_3 = x_3.B(x_2)$. $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash x_3 : \{B(r) : T_5..T_6\}$. $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash [x_2/r]T_6$ **ro** $T_1$. $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash [x_2/r]T_6$ $\mathbf{mu}(r_1)$ $T_4$.

  By induction on variable typing and splitting, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3 : [y/w]\{B(r) : T_5..T_6\}$, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w][x_2/r]T_6$ **ro** $[y/w]T_1$, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w][x_2/r]T_6$ $\mathbf{mu}(r_1)$ $[y/w]T_4$.

By (TX-Typ), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3 : \{B(r) : [y/w]T_5..[y/w]T_6\}$. By 5.21(SubSwap), $\Gamma_1, [y/w]\Gamma_2;$ $\rho_1, \rho_2 \vdash [[y/w]x_2/r][y/w]T_6 \ \mathbf{ro}\ [y/w]T_1$, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [[y/w]x_2/r][y/w]T_6 \ \mathbf{mu}(r_1)\ [y/w]T_4$. By (TS-Sel), $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3.B([y/w]x_2)\ \mathbf{ro}\ [y/w]T_1$, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]x_3.B([y/w]x_2)\ \mathbf{mu}(r_1)\ [y/$
By (TX-Sel).

- Case (TS-AndR): $T_3 = T_5 \wedge T_6$, and $T_1 = T_7 \wedge T_8$, where $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_5\ \mathbf{ro}\ T_7$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_6\ \mathbf{ro}\ T_8$.

  By induction on splitting, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_5\ \mathbf{ro}\ [y/w]T_7$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_6\ \mathbf{ro}\ [y/w]T_8$. By (TS-AndR) and (TX-And).

- Case (TS-AndM): $T_3 = T_5 \wedge T_6$, and $T_4 = T_7 \wedge T_8$, where $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_5\ \mathbf{mu}(r_1)\ T_7$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_6\ \mathbf{mu}(r_1)\ T_8$.

  By induction on splitting, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_5\ \mathbf{mu}(r_1)\ [y/w]T_7$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_6\ \mathbf{mu}(r_1)\ [y/w]T_8$. By (TS-AndM) and (TX-And).

- Case (TS-OrR): $T_3 = T_5 \vee T_6$, and $T_1 = T_7 \vee T_8$, where $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_5\ \mathbf{ro}\ T_7$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_6\ \mathbf{ro}\ T_8$.

  By induction on splitting, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_5\ \mathbf{ro}\ [y/w]T_7$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_6\ \mathbf{ro}\ [y/w]T_8$. By (TS-OrR) and (TX-Or).

- Case (TS-OrM): $T_3 = T_5 \vee T_6$, and $T_4 = T_7 \vee T_8$, where $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_5\ \mathbf{mu}(r_1)\ T_7$, and $\Gamma_1, w : T_2, \Gamma_2;\rho_1, w \to y, \rho_2 \vdash T_6\ \mathbf{mu}(r_1)\ T_8$.

  By induction on splitting, $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_5\ \mathbf{mu}(r_1)\ [y/w]T_7$, and $\Gamma_1, [y/w]\Gamma_2;\rho_1, \rho_2 \vdash [y/w]T_6\ \mathbf{mu}(r_1)\ [y/w]T_8$. By (TS-OrM) and (TX-Or).

□

Finally the variant 5.33(SubR) shows that a free variable can be replaced by any variable

**Lemma 5.33** (SubR). *The following holds for variable typing, subtyping, splitting :*

- *If* $\Gamma;\rho \vdash x_1 : T_1$, *and* $u \notin \Gamma$ *and* $u \notin \rho$, *then* $\Gamma;\rho \vdash [x/u]x_1 : [x/u]T_1$.
- *If* $\Gamma;\rho \vdash T_3 <: T_1$, *and* $u \notin \Gamma$ *and* $u \notin \rho$, *then* $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_1$.
- *If* $\Gamma;\rho \vdash T_3\ \mathbf{ro}\ T_1$, *and* $u \notin \Gamma$ *and* $u \notin \rho$, *then* $\Gamma;\rho \vdash [x/u]T_3\ \mathbf{ro}\ [x/u]T_1$.
- *If* $\Gamma;\rho \vdash T_3\ \mathbf{mu}(r_1)\ T_4$, *and* $u \neq r_1$, *and* $u \notin \Gamma$ *and* $u \notin \rho$, *then* $\Gamma;\rho \vdash [x/u]T_3\ \mathbf{mu}(r_1)\ [x/u]T_4$.

*Proof.* Induction on variable typing, subtyping, splitting:

- Case (VT-Var): $\Gamma = \Gamma_3, x_1 : T_1, \Gamma_4$, where $x_1 \notin \text{dom}\ \Gamma_4$. Because $u \notin \Gamma$, therefore $x_1 \neq u$, and $u \notin T_1$, therefore $[x/u]x_1 = x_1$, and $[x/u]T_1 = T_1$.
- Case (VT-RecE): $T_1 = [x_1/s]T_4$, and $\Gamma;\rho \vdash x_1 : \mu(s : T_4)$, and $T_4\ \mathbf{indep}\ s$. Using alpha-equivalence, assume that $s \neq x$.

  By induction on variable typing, $\Gamma;\rho \vdash [x/u]x_1 : \mu(s : [x/u]T_4)$. By 5.25(SubIndep), $[x/u]T_4\ \mathbf{indep}\ s$. By (VT-RecE), $\Gamma;\rho \vdash [x/u]x_1 : [[x/u]x_1/s][x/u]T_4$. By 5.21(SubSwap), $[[x/u]x_1/s][x/u]T_4 = [x/u]T_1$.

- Case (VT-RecI): $\Gamma;\rho \vdash x_1 : [x_1/s]T_4$, and $T_1 = \mu(s : T_4)$, and $\Gamma;\rho \vdash [x_1/s]T_4\ \mathbf{ro}\ [x_1/s]T_4$, and $T_4\ \mathbf{indep}\ s$. Using alpha-equivalence, assume that $s \neq x$.

  By induction on ro splitting, $\Gamma;\rho \vdash [x/u][x_1/s]T_4\ \mathbf{ro}\ [x/u][x_1/s]T_4$. By induction on variable typing, $\Gamma;\rho \vdash [x/u]x_1 : [x/u][x_1/s]T_4$. By 5.21(SubSwap), $[x/u][x_1/s]T_4 = [[x/u]x_1/s][x/u]T_4$. By 5.25(SubIndep), $[x/u]T_4\ \mathbf{indep}\ s$. By (VT-RecI), $\Gamma;\rho \vdash [x/u]x_1 : \mu(s : [x/u]T_4)$.

- Case (VT-AndI): $T_1 = T_4 \wedge T_5$, and $\Gamma;\rho \vdash x_1 : T_4$, and $\Gamma;\rho \vdash x_1 : T_5$. By induction on variable typing, $\Gamma;\rho \vdash [x/u]x_1 : [x/u]T_4$, and $\Gamma;\rho \vdash [x/u]x_1 : [x/u]T_5$. By (VT-AndI) and (TX-And), $\Gamma;$ $\rho \vdash [x/u]x_1 : [x/u]T_1$.
- Case (VT-MutTop): $T_1 = \{\mathsf{M}(r_0) : \bot..\top\}$. Directly by (VT-MutTop) and (TX-Top) and (TX-Bot) and (TX-Typ).
- Case (VT-Sub): $\Gamma;\rho \vdash x_1 : T_4$. $\Gamma;\rho \vdash T_4 <: T_1$. By induction on variable typing, $\Gamma;\rho \vdash [x/u]x_1 :$ $[x/u]T_4$. By induction on subtyping, $\Gamma;\rho \vdash [x/u]T_4 <: [x/u]T_1$. By (VT-Sub), $\Gamma;\rho \vdash [x/u]x_1 :$ $[x/u]T_1$.

- Case (ST-Top): $T_1 = \top$. Directly by (ST-Top) and (TX-Top).
- Case (ST-Bot): $T_3 = \bot$. Directly by (ST-Bot) and (TX-Bot).
- Case (ST-Refl): $T_3 = T_1$. Directly by (ST-Refl).
- Case (ST-And1): $T_3 = T_1 \wedge T_4$. By (ST-And1), $\Gamma;\rho \vdash [x/u]T_4 \wedge [x/u]T_1 <: [x/u]T_1$. By (TX-And).
- Case (ST-And2): $T_3 = T_4 \wedge T_1$. By (ST-And2), $\Gamma;\rho \vdash [x/u]T_4 \wedge [x/u]T_1 <: [x/u]T_1$. By (TX-And).
- Case (ST-And): $T_1 = T_4 \wedge T_5$, and $\Gamma;\rho \vdash T_3 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_5$. By induction on subtyping, $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_4$, $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_5$. By (ST-And), $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_4 \wedge [x/u]T_5$. By (TX-And).
- Case (ST-Or1): $T_1 = T_3 \vee T_4$. By (ST-Or1), $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_3 \vee [x/u]T_4$. By (TX-Or).
- Case (ST-Or2): $T_1 = T_4 \vee T_3$. By (ST-Or2), $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_4 \vee [x/u]T_3$. By (TX-Or).
- Case (ST-Or): $T_3 = T_4 \vee T_5$, and $\Gamma;\rho \vdash T_4 <: T_1$, and $\Gamma;\rho \vdash T_5 <: T_1$. By induction on subtyping, $\Gamma;\rho \vdash [x/u]T_4 <: [x/u]T_1$, $\Gamma;\rho \vdash [x/u]T_5 <: [x/u]T_1$. By (ST-Or), $\Gamma;\rho \vdash [x/u]T_4 \vee [x/u]T_5 <: [x/u]T_1$. By (TX-Or).
- Case (ST-Trans): $\Gamma;\rho \vdash T_3 <: T_4$, and $\Gamma;\rho \vdash T_4 <: T_1$.

  By induction on subtyping, $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_4$, and $\Gamma;\rho \vdash [x/u]T_4 <: [x/u]T_1$. By (ST-Trans), $\Gamma;\rho \vdash [x/u]T_3 <: [x/u]T_1$.
- Case (ST-SelL): $T_3 = [x_2/r]T_4$, and $T_1 = x_3.B(x_2)$, and $\Gamma;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$.

  Similarly as (ST-SelU). By induction on variable typing, $\Gamma;\rho \vdash [x/u]x_3 : [x/u]\{B(r) : T_4..T_5\}$. By (TX-Typ), $\Gamma;\rho \vdash [x/u]x_3 : \{B(r) : [x/u]T_4..[x/u]T_5\}$. By (ST-SelL), $\Gamma;\rho \vdash [[x/u]x_2/r][x/u]T_4 <: [x/u]x_3.B([x/u]x_2)$. By 5.21(SubSwap) and (TX-Sel), $\Gamma;\rho \vdash [x/u][x_2/r]T_4 <: [x/u]x_3.B(x_2)$.
- Case (ST-SelU): $T_3 = x_3.B(x_2)$, and $T_1 = [x_2/r]T_5$, and $\Gamma;\rho \vdash x_3 : \{B(r) : T_4..T_5\}$.

  By induction on variable typing, $\Gamma;\rho \vdash [x/u]x_3 : [x/u]\{B(r) : T_4..T_5\}$. By (TX-Typ), $\Gamma;\rho \vdash [x/u]x_3 : \{B(r) : [x/u]T_4..[x/u]T_5\}$. By (ST-SelU), $\Gamma;\rho \vdash [x/u]x_3.B([x/u]x_2) <: [[x/u]x_2/r][x/u]T_5$. By 5.21(SubSwap) and (TX-Sel), $\Gamma;\rho \vdash [x/u]x_3.B(x_2) <: [x/u][x_2/r]T_5$.
- Case (ST-TypAnd): $T_3 = \{B(r) : T_4..T_5\} \wedge \{B(r) : T_6..T_7\}$, and $T_1 = \{B(r) : T_4 \vee T_6..T_5 \wedge T_7\}$. By (ST-TypAnd) and (TX-And) and (TX-Or) and (TX-Typ).
- Case (ST-Dist): $T_3 = T_4 \wedge (T_5 \vee T_6)$. $T_1 = (T_4 \wedge T_5) \vee (T_4 \wedge T_6)$. By (ST-Dist) and (TX-Or) and (TX-And).
- Case (ST-Typ): $T_3 = \{B(r) : T_4..T_5\}$, and $T_1 = \{B(r) : T_6..T_7\}$, where $\Gamma;\rho \vdash T_6 <: T_4$, and $\Gamma;\rho \vdash T_5 <: T_7$. Using alpha-equivalence, assume that $u$, $x$ are disjoint from $r$.

  By induction on subtyping, $\Gamma;\rho \vdash [x/u]T_6 <: [x/u]T_4$, and $\Gamma;\rho \vdash [x/u]T_5 <: [x/u]T_7$. By (ST-Typ) and (TX-Typ).
- Case (ST-Fld): $T_3 = \{a : T_4..T_5\}$, and $T_1 = \{a : T_6..T_7\}$, where $\Gamma;\rho \vdash T_6 <: T_4$, and $\Gamma;\rho \vdash T_5 <: T_7$.

  By induction on subtyping, $\Gamma;\rho \vdash [x/u]T_6 <: [x/u]T_4$, and $\Gamma;\rho \vdash [x/u]T_5 <: [x/u]T_7$. By (ST-Fld) and (TX-Fld).
- Case (ST-Met): $T_3 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, where $\Gamma;\rho \vdash T_7 <: T_4$, and $\Gamma, z : T_7;\rho \vdash T_9 <: T_6$, and $\Gamma, z : T_7, r : T_9;\rho \vdash T_5 <: T_8$. Using alpha-equivalence, assume that $u$, $x$ are disjoint from $r$ and $z$.

  By induction on subtyping, $\Gamma;\rho \vdash [x/u]T_7 <: [x/u]T_4$. By induction on subtyping, $\Gamma, z : [x/u]T_7;\rho \vdash [x/u]T_9 <: [x/u]T_6$, and $\Gamma, z : [x/u]T_7, r : [x/u]T_9;\rho \vdash [x/u]T_5 <: [x/u]T_8$. By (ST-Met) and (TX-Met).
- Case (ST-Eq): $\rho \vdash T_3 \approx T_1$. By 5.26(SubEq), $\rho \vdash [x/u]T_3 \approx [x/u]T_1$. By (ST-Eq).
- Case (ST-N-M): $T_3 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_1 = \bot$. By (ST-N-M) and (TX-Bot) and (TX-Typ) and (TX-N) and (TX-And).
- Case (ST-N-Rec): $T_3 = \mathsf{N}$, and $T_1 = \mu(s : T_4)$. Using alpha-equivalence, assume that $u$, $x$ are disjoint from $s$. By (ST-N-Rec) and (TX-Rec) and (TX-N).
- Case (ST-N-Fld): $T_3 = \mathsf{N}$, and $T_1 = \{a : T_6..T_7\}$. By (ST-N-Fld) and (TX-Fld) and (TX-N).
- Case (ST-N-Met): $T_3 = \mathsf{N}$, and $T_1 = \{m(z : T_7, r : T_9) : T_8\}$. Using alpha-equivalence, assume that $u$, $x$ are disjoint from $r$ and $z$. By (ST-N-Met) and (TX-Met) and (TX-N).

- Case (ST-N-Typ): $T_3 = \mathsf{N}$, and $T_1 = \{B(r) : T_6..T_7\}$. Using alpha-equivalence, assume that $u$, $x$ are disjoint from $r$. By (ST-N-Typ) and (TX-Typ) and (TX-N).
- Case (TS-Top): $T_3 = \top$, and $T_1 = \top$, and $T_4 = \top$. By (TS-Top) and (TX-Top).
- Case (TS-Bot): $T_3 = \bot$, and $T_1 = \mathsf{N}$, and $T_4 = \bot$. By (TS-Bot) and (TX-Bot) and (TX-N).
- Case (TS-M): $T_3 = \{\mathsf{M}(r_1) : T_5..T_4\}$, and $T_1 = \top$. By (TS-M) and (TX-Typ).
- Case (TS-Typ): By (TS-Typ).
- Case (TS-Fld): By (TS-Fld).
- Case (TS-Met): By (TS-Met).
- Case (TS-Rec): By (TS-Rec).
- Case (TS-Sel): $T_3 = x_3.B(x_2)$. $\Gamma;\rho \vdash x_3 : \{B(r) : T_5..T_6\}$. $\Gamma;\rho \vdash [x_2/r]T_6$ **ro** $T_1$. $\Gamma;\rho \vdash [x_2/r]T_6$ $\mathbf{mu}(r_1)$ $T_4$.

  By induction on variable typing and splitting, $\Gamma;\rho \vdash [x/u]x_3 : [x/u]\{B(r) : T_5..T_6\}$, $\Gamma;\rho \vdash [x/u][x_2/r]T_6$ **ro** $[x/u]T_1$, $\Gamma;\rho \vdash [x/u][x_2/r]T_6$ $\mathbf{mu}(r_1)$ $[x/u]T_4$. By (TX-Typ), $\Gamma;\rho \vdash [x/u]x_3 : \{B(r) : [x/u]T_5..[x/u]T_6\}$. By 5.21(SubSwap), $\Gamma;\rho \vdash [[x/u]x_2/r][x/u]T_6$ **ro** $[x/u]T_1$, $\Gamma;\rho \vdash [[x/u]x_2/r][x/u]T_6$ $\mathbf{mu}(r_1)$ $[x/u]T_4$. By (TS-Sel), $\Gamma;\rho \vdash [x/u]x_3.B([x/u]x_2)$ **ro** $[x/u]T_1$, $\Gamma;\rho \vdash [x/u]x_3.B([x/u]x_2)$ $\mathbf{mu}(r_1)$ $[x/u]T_4$. By (TX-Sel).
- Case (TS-AndR): $T_3 = T_5 \wedge T_6$, and $T_1 = T_7 \wedge T_8$, where $\Gamma;\rho \vdash T_5$ **ro** $T_7$, and $\Gamma;\rho \vdash T_6$ **ro** $T_8$.

  By induction on splitting, $\Gamma;\rho \vdash [x/u]T_5$ **ro** $[x/u]T_7$, and $\Gamma;\rho \vdash [x/u]T_6$ **ro** $[x/u]T_8$. By (TS-AndR) and (TX-And).
- Case (TS-AndM): $T_3 = T_5 \wedge T_6$, and $T_4 = T_7 \wedge T_8$, where $\Gamma;\rho \vdash T_5$ $\mathbf{mu}(r_1)$ $T_7$, and $\Gamma;\rho \vdash T_6$ $\mathbf{mu}(r_1)$ $T_8$.

  By induction on splitting, $\Gamma;\rho \vdash [x/u]T_5$ $\mathbf{mu}(r_1)$ $[x/u]T_7$, and $\Gamma;\rho \vdash [x/u]T_6$ $\mathbf{mu}(r_1)$ $[x/u]T_8$. By (TS-AndM) and (TX-And).
- Case (TS-OrR): $T_3 = T_5 \vee T_6$, and $T_1 = T_7 \vee T_8$, where $\Gamma;\rho \vdash T_5$ **ro** $T_7$, and $\Gamma;\rho \vdash T_6$ **ro** $T_8$.

  By induction on splitting, $\Gamma;\rho \vdash [x/u]T_5$ **ro** $[x/u]T_7$, and $\Gamma;\rho \vdash [x/u]T_6$ **ro** $[x/u]T_8$. By (TS-OrR) and (TX-Or).
- Case (TS-OrM): $T_3 = T_5 \vee T_6$, and $T_4 = T_7 \vee T_8$, where $\Gamma;\rho \vdash T_5$ $\mathbf{mu}(r_1)$ $T_7$, and $\Gamma;\rho \vdash T_6$ $\mathbf{mu}(r_1)$ $T_8$.

  By induction on splitting, $\Gamma;\rho \vdash [x/u]T_5$ $\mathbf{mu}(r_1)$ $[x/u]T_7$, and $\Gamma;\rho \vdash [x/u]T_6$ $\mathbf{mu}(r_1)$ $[x/u]T_8$. By (TS-OrM) and (TX-Or).

□

### 5.1.6 Splitting lemmata

This section contains properties of the type splitting relations $\vdash \quad \mathbf{ro}$ and $\vdash \quad \mathbf{mu}()$ , defined in Section 3.10. The splitting operations split a type into a read-only and mutability part. The read-only part is an immutable supertype of the original type.

The lemmata 5.34(ROSub) and 5.35(MUSub) show that the splitting operations give use an upper bound for the type and its mutability. The lemma 5.36(SplitSub) shows how splitting a type into the read-only part and mutability can be used to construct the form that is used in the conclusion of the (TT-Read) rule.

**Lemma 5.34** (ROSub). *If* $\Gamma;\rho \vdash T_1$ $\mathbf{ro}$ $T_2$*, then* $\Gamma;\rho \vdash T_1 <: T_2$.

*Idea.* The read-only version of a type is a supertype of the original type. ▽

*Proof.* Induction on $\Gamma;\rho \vdash T_1$ $\mathbf{ro}$ $T_2$:

- Case (TS-Top): $T_2 = \top$. By (ST-Top).
- Case (TS-Bot): $T_1 = \bot$. By (ST-Bot).
- Case (TS-M): $T_2 = \top$. By (ST-Top).
- Cases (TS-Typ), (TS-Met), (TS-Fld), (TS-Rec): $T_1 = T_2$. By (ST-Refl).
- Case (TS-Sel): $T_1 = x_1.B(x_2)$. $\Gamma;\rho \vdash x : \{B(r) : T_3..T_4\}$. $\Gamma;\rho \vdash [x_2/r]T_4$ $\mathbf{ro}$ $T_2$. By induction, $\Gamma;\rho \vdash [x_2/r]T_4 <: T_2$. By (ST-SelU), $\Gamma;\rho \vdash T_1 <: [x_2/r]T_4$. By (ST-Trans), $\Gamma;\rho \vdash T_1 <: T_2$.
- Case (TS-AndR): $T_1 = T_3 \wedge T_4$. $T_2 = T_5 \wedge T_6$. $\Gamma;\rho \vdash T_3$ $\mathbf{ro}$ $T_5$. $\Gamma;\rho \vdash T_4$ $\mathbf{ro}$ $T_6$. By induction, $\Gamma;\rho \vdash T_3 <: T_5$, and $\Gamma;\rho \vdash T_4 <: T_6$. By 5.18(AndSub), $\Gamma;\rho \vdash T_3 \wedge T_4 <: T_5 \wedge T_6$.
- Case (TS-OrR): $T_1 = T_3 \vee T_4$. $T_2 = T_5 \vee T_6$. $\Gamma;\rho \vdash T_3$ $\mathbf{ro}$ $T_5$. $\Gamma;\rho \vdash T_4$ $\mathbf{ro}$ $T_6$. By induction, $\Gamma;\rho \vdash T_3 <: T_5$, and $\Gamma;\rho \vdash T_4 <: T_6$. By 5.19(OrSub), $\Gamma;\rho \vdash T_3 \vee T_4 <: T_5 \vee T_6$.

□

**Lemma 5.35** (MUSub). *If* $\Gamma;\rho \vdash T_1$ $\mathbf{mu}(r_0)$ $T_2$*, then* $\Gamma;\rho \vdash \top <: T_2$ *or* $\Gamma;\rho \vdash T_1 <: \{\mathsf{M}(r_0) : \bot..T_2\}$.

*Proof.* Induction on $\Gamma;\rho \vdash T_1$ $\mathbf{mu}(r_0)$ $T_2$:

- Case (TS-Top): $T_2 = \top$. By (ST-Refl), $\Gamma;\rho \vdash \top <: T_2$.
- Case (TS-Bot): $T_1 = \bot$. By (ST-Bot), $\Gamma;\rho \vdash \bot <: \{\mathsf{M}(r_0) : \bot..\bot\}$.
- Case (TS-M): $T_1 = \{\mathsf{M}(r) : T_3..T_2\}$. By (ST-Bot), $\Gamma;\rho \vdash \bot <: T_3$. By (ST-Typ), $\Gamma;\rho \vdash \{\mathsf{M}(r) : T_1..T_2\} <: \{\mathsf{M}(r_0) : \bot..T_2\}$.
- Cases (TS-Typ), (TS-Met), (TS-Fld), (TS-Rec): $T_2 = \top$. By (ST-Refl).
- Case (TS-Sel): $T_1 = x_1.B(x_2)$. $\Gamma;\rho \vdash x_1 : \{B(r) : T_3..T_4\}$. $\Gamma;\rho \vdash [x_2/r]T_4$ $\mathbf{mu}(r_0)$ $T_2$. By (ST-SelU), $\Gamma;\rho \vdash T_1 <: [x_2/r]T_4$. By induction, $\Gamma;\rho \vdash \top <: T_2$, or $\Gamma;\rho \vdash [x_2/r]T_4 <: \{\mathsf{M}(r_0) : \bot..T_2\}$. Unless $\Gamma;\rho \vdash \top <: T_2$, by (ST-Trans), $\Gamma;\rho \vdash T_1 <: \{\mathsf{M}(r_0) : \bot..T_2\}$.
- Case (TS-AndM): $T_1 = T_3 \wedge T_4$. $T_2 = T_5 \wedge T_6$. $\Gamma;\rho \vdash T_3$ $\mathbf{mu}(r_0)$ $T_5$. $\Gamma;\rho \vdash T_4$ $\mathbf{mu}(r_0)$ $T_6$. By induction, $\Gamma;\rho \vdash T_3 <: \{\mathsf{M}(r_0) : \bot..T_5\}$, or $\Gamma;\rho \vdash \top <: T_5$. By induction, $\Gamma;\rho \vdash T_4 <: \{\mathsf{M}(r_0) : \bot..T_6\}$, or $\Gamma;\rho \vdash \top <: T_6$. If $\Gamma;\rho \vdash \top <: T_5$, and $\Gamma;\rho \vdash \top <: T_6$, then by (ST-And), $\Gamma;\rho \vdash \top <: T_2$. If $\Gamma;\rho \vdash \top <: T_5$, then by (ST-Top) and (ST-Trans), $\Gamma;\rho \vdash T_6 <: T_5$. By (ST-Refl) and (ST-And), $\Gamma;\rho \vdash T_6 <: T_5 \wedge T_6$. By (ST-And2), $T_3 \wedge \Gamma;\rho \vdash T_4 <: T_4$. By (ST-Typ) and (ST-Trans), $\Gamma;\rho \vdash T_3 \wedge T_4 <: \{\mathsf{M}(r_0) : \bot..T_5 \wedge T_6\}$. If $\Gamma;\rho \vdash \top <: T_6$, then by (ST-Top) and (ST-Trans), $\Gamma;\rho \vdash T_5 <: T_6$. By (ST-Refl) and (ST-And), $\Gamma;\rho \vdash T_5 <: T_5 \wedge T_6$. By (ST-And1), $T_3 \wedge \Gamma;\rho \vdash T_4 <: T_3$. By (ST-Typ) and (ST-Trans), $\Gamma;\rho \vdash T_3 \wedge T_4 <: \{\mathsf{M}(r_0) : \bot..T_5 \wedge T_6\}$. Otherwise, by (ST-TypAnd), $\Gamma;\rho \vdash T_3 \wedge T_4 <: \{\mathsf{M}(r_0) : \bot..T_5 \wedge T_6\}$.
- Case (TS-OrM): $T_1 = T_3 \vee T_4$. $T_2 = T_5 \vee T_6$. $\Gamma;\rho \vdash T_3$ $\mathbf{mu}(r_0)$ $T_5$. $\Gamma;\rho \vdash T_4$ $\mathbf{mu}(r_0)$ $T_6$. By induction, $\Gamma;\rho \vdash T_3 <: \{\mathsf{M}(r_0) : \bot..T_5\}$, or $\Gamma;\rho \vdash \top <: T_5$. By induction, $\Gamma;\rho \vdash T_4 <: \{\mathsf{M}(r_0) : \bot..T_6\}$, or $\Gamma;\rho \vdash \top <: T_6$. If $\Gamma;\rho \vdash \top <: T_5$, then by (ST-Or1) and (ST-Trans), $\Gamma;\rho \vdash \top <: T_2$. If $\Gamma;\rho \vdash \top <: T_6$, then by (ST-Or2) and (ST-Trans), $\Gamma;\rho \vdash \top <: T_2$. Otherwise, by 5.20(OrTypSub), $\Gamma;\rho \vdash T_3 \vee T_4 <: \{\mathsf{M}(r_0) : \bot..T_5 \vee T_6\}$.

□

**Lemma 5.36** (SplitSub). *If* $\Gamma;\rho \vdash x : T_1$*, and* $\Gamma;\rho \vdash T_1\ \mathbf{ro}\ T_2$*, and* $\Gamma;\rho \vdash T_1\ \mathbf{mu}(r_0)\ T_3$*, then* $\Gamma;\rho \vdash x : T_2 \wedge \{\mathsf{M}(r_0) : \bot..(T_3 \vee T_4)\}$.

*Proof.* By 5.34(ROSub), $\Gamma;\rho \vdash T_1 <: T_2$. By (VT-Sub), $\Gamma;\rho \vdash x : T_2$. By 5.35(MUSub), $\Gamma;\rho \vdash T_1 <: \{\mathsf{M}(r_0) : \bot..T_3\}$, or $\Gamma;\rho \vdash \top <: T_3$. By (ST-Or), $\Gamma;\rho \vdash T_3 <: T_3 \vee T_4$. By (ST-Typ), $\Gamma;\rho \vdash \{\mathsf{M}(r_0) : \bot..T_3\} <: \{\mathsf{M}(r_0) : \bot..(T_3 \vee T_4)\}$.

If $\Gamma;\rho \vdash T_1 <: \{\mathsf{M}(r_0) : \bot..T_3\}$, then by (VT-Sub), $\Gamma;\rho \vdash x : \{\mathsf{M}(r_0) : \bot..(T_3 \vee T_4)\}$. Otherwise, $\Gamma;\rho \vdash \top <: T_3$. By (VT-MutTop), $\Gamma;\rho \vdash x : \{\mathsf{M}(r_0) : \bot..\top\}$. By (ST-Typ), $\Gamma;\rho \vdash \{\mathsf{M}(r_0) : \bot..\top\} <: \{\mathsf{M}(r_0) : \bot..T_3\}$. By (VT-Sub), $\Gamma;\rho \vdash x : \{\mathsf{M}(r_0) : \bot..T_3\}$. By (VT-Sub), $\Gamma;\rho \vdash x : \{\mathsf{M}(r_0) : \bot..(T_3 \vee T_4)\}$. By (VT-AndI), $\Gamma;\rho \vdash x : T_2 \wedge \{\mathsf{M}(r_0) : \bot..(T_3 \vee T_4)\}$. □

**Lemma 5.37** (RecordRO). *If* $\Gamma;\rho \vdash R_1\ \mathbf{ro}\ R_2$*, then* $R_2 = R_1$.

*Idea.* Read-only version of a record type is the same type. ▽

*Proof.* Induction on $R_1$:

- If $R_1 = R_3 \wedge R_4$. By inversion of (TS-AndR), $R_2 = R_5 \wedge R_6$, where $\Gamma;\rho \vdash R_3\ \mathbf{ro}\ R_4$, and $\Gamma;\rho \vdash R_5\ \mathbf{ro}\ R_6$. By induction, $R_5 = R_3$, and $R_6 = R_4$.
- If $R_1 = \{a : T_1..T_1\}$. By inversion of (TS-Fld), $R_2 = R_1$.
- If $R_1 = \{A(r) : T_1..T_2\}$. By inversion of (TS-Typ), $R_2 = R_1$.
- If $R_1 = \{m(z : T_1, r : T_3) : T_2\}$. By inversion of (TS-Met), $R_2 = R_1$.

□

## 5.2 Runtime lemmata

This section states properties related to machine configurations and their reduction.

### 5.2.1 T-Free Variables Lemmata

The following lemmata state that in a term, there are no unexpected locations, which correspond to an object on the heap. However, this only holds for occurrences outside of a type, because defining a method which takes a parameter of type $y.A(x)$ is allowed even though $y$ does not exist.

**Lemma 5.38** (TVC). *If* $\Gamma;\rho \vdash x : T$*, then* $x \in \mathrm{dom}\ \Gamma$*.*

*Proof.* Induction on variable typing:

- Case (VT-Var): Rule requires $x \in \mathrm{dom}\ \Gamma$.
- Cases (VT-RecE), (VT-RecI), (VT-AndI), (VT-MutTop), (VT-Sub): All these rules have a premise of the form $\Gamma;\rho \vdash x : T_1$. By induction.

□

**Lemma 5.39** (FVC). *If* $\Gamma;\rho \vdash t : T$*, and* $t$ $\mathbf{tfree}$ $x$*, then* $x \in \mathrm{dom}\ \Gamma$*. If* $\Gamma;\rho \vdash d : T$*, and* $d$ $\mathbf{tfree}$ $x$*, then* $x \in \mathrm{dom}\ \Gamma$*.*

*Proof.* Induction on on term and definition typing:

- Cases (TT-Var), (TT-Apply), (TT-Read), (TT-Write): By 5.38(TVC).
- Case (TT-New): If $x = z$, then there are no free occurrences in $t$. Otherwise by induction on term typing. If $x = s$, then there are no free occurrences in $d$. Otherwise by induction on definition typing.
- Case (TT-Let): occurrences in $t_1$ by induction. If $x = z$, then there are no free occurrences in $t_2$. Otherwise by induction on term typing.
- Case (TT-Sub): By induction on term typing.
- Cases (DT-Typ), (DT-TypB): no t-free occurrences.
- Case (DT-Fld): By 5.38(TVC).
- Case (DT-And): By induction on definition typing.
- Case (DT-Met): If $x = z$, then there are no free occurrences in $t_2$. If $x = s$, then there are also no free occurrences in $t_2$, because the method definition can only be typed inside $\nu(s : T_1)d$. Otherwise by induction on term typing.

□

**Lemma 5.40** (SFVC). *If* $\mathrm{F};\rho \vdash \sigma : T_1, T_2$*, and* $\sigma$ $\mathbf{tfree}$ $x$*, then* $x \in \mathrm{dom}\ \mathrm{F}$*.*

*Proof.* Induction on stack typing:

- Case (CT-EmptyS): No occurrences.
- Case (CT-LetS): Occurrences in $\sigma$ by induction. If $x = z$, then there are no t-free occurrences. Otherwise, by 5.39(FVC).

□

**Lemma 5.41** (RFV). *If* $\mathrm{F};\rho \vdash \langle t; \sigma; \rho; \Sigma\rangle : T$*, then all t-free variables in t and* $\sigma$ *are references.*

*Proof.* By 5.39(FVC), all t-free variables in $t$ are in $\mathrm{dom}\ \mathrm{F}$. By 5.40(SFVC), the same for t-free variables in $s$. Because F is inert, all such variables are references of locations. Configuration typing requires that there are no locations in $t$ and $s$. □

**Lemma 5.42** (IFV). *If* $\mathrm{F};\rho \vdash \langle t; \cdot; \rho; \cdot\rangle : T$*, then t has no t-free variables.*

*Proof.* By 5.39(FVC), all t-free variables in $t$ are in $\mathrm{dom}\ \mathrm{F}$. By configuration typing, heap correspondence and runtime environment correspondence, they also have a corresponding locatoin on the heap. Because the heap is empty, there are no such variables. □

Locations cannot appear in the body of a method. This is required because otherwise a read-only method of an object could modify captured variables. This is achieved by variable visibility.

**Lemma 5.43** (VVE). *If* $\Gamma, x_2 : T$ **vis** $x_1$*, and* $x_1 \neq x_2$*, then* $\Gamma$ **vis** $x_1$*.*

*Proof.* By inversion of (Vis-Var), $\Gamma, x_2 : T = \Gamma_1, x_1 : T_1, \Gamma_2$, and $! \notin \Gamma_2$. Because $x_1 \neq x_2$, $\Gamma_2 = \Gamma_3, x_2 : T$, and $\Gamma = \Gamma_1, x_1 : T_1, \Gamma_3$, and $! \notin \Gamma_3$. By (Vis-Var). □

**Lemma 5.44** (VFV). *If* $\Gamma;\rho \vdash t : T$*, and* $t$ **tfree** $x$*, then* $\Gamma$ **vis** $x$*. If* $\Gamma;\rho \vdash d : T$*, and* $d$ **tfree** $x$*, then* $\Gamma$ **vis** $x$*.*

*Idea.* If a variable is t-free in a typed term or definition, then it must be visible in the typing context. ▽

*Proof idea.* Induction on t-free variable. Rules for typing terms and definitions containing variables require visibility. ▽

*Proof.* Induction on $t$ **tfree** $x$:

- Case (TF-Var): $t = \mathsf{v}x$. By inversion of (TT-Var), $\Gamma$ **vis** $x$.
- Case (TF-Apply1): $t = x.m\, x_2$. By inversion of (TT-Apply), $\Gamma$ **vis** $x$.
- Case (TF-Apply1): $t = x_1.m\, x$. By inversion of (TT-Apply), $\Gamma$ **vis** $x$.
- Case (TF-Read): $t = x.a$. By inversion of (TT-Read), $\Gamma$ **vis** $x$.
- Case (TF-Write1): $t = x.a := x_2$. By inversion of (TT-Write), $\Gamma$ **vis** $x$.
- Case (TF-Write2): $t = x_1.a := x$. By inversion of (TT-Write), $\Gamma$ **vis** $x$.
- Case (TF-NewD): $t = \mathsf{let}\ z = \nu(s : T_1)d\ \mathsf{in}\ t$. $d$ **tfree** $x$. $x \neq s$. By inversion of (TT-New), $\Gamma, s : T_1; \rho \vdash d : T_1$. By induction, $\Gamma, s : T_1$ **vis** $x$. By 5.43(VVE), $\Gamma$ **vis** $x$.
- Case (TF-NewT): $t = \mathsf{let}\ z = \nu(s : T_1)d\ \mathsf{in}\ t$. $t$ **tfree** $x$. $x \neq z$. By inversion of (TT-New), $\Gamma, z : T_3; \rho \vdash t : T_2$. By induction, $\Gamma, z : T_3$ **vis** $x$. By 5.43(VVE), $\Gamma$ **vis** $x$.
- Case (TF-LetPush): $t = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$. $t_1$ **tfree** $x$. By inversion of (TT-Let), $\Gamma;\rho \vdash t_1 : T_1$. By induction, $\Gamma$ **vis** $x$.
- Case (TF-LetPop): $t = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$. $t_2$ **tfree** $x$. $x \neq z$. By inversion of (TT-Let), $\Gamma, z : T_1; \rho \vdash t_2 : T_2$. By induction, $\Gamma, z : T_1$ **vis** $x$. By 5.43(VVE), $\Gamma$ **vis** $x$.
- Case (TF-Fld): $d = \{a = x_1\}$, and $\Gamma$ **vis** $x_1$. The t-free occurence is $x_1$ by (TF-Fld), so $x = x_1$.
- Case (TF-Met): $d = \{m(z, r) = t\}$. $t$ **tfree** $x$. $x \neq z$. $x \neq r$. By inversion of (DT-Met), $\Gamma, !, r : T_3, z : T_1;\rho \vdash t : T_2$. By induction, $\Gamma, !, r : T_3, z : T_1$ **vis** $x$. By 5.43(VVE) twice, $\Gamma, !$ **vis** $x$. By 5.14(Unhide), $\Gamma$ **vis** $x$.
- Case (TF-And1): $d = d_1 \wedge d_2$. $d_1$ **tfree** $x$. By inversion of (DT-And), $\Gamma;\rho \vdash d_1 : T_1$. By induction, $\Gamma$ **vis** $x$.
- Case (TF-And2): $d = d_1 \wedge d_2$. $d_2$ **tfree** $x$. By inversion of (DT-And), $\Gamma;\rho \vdash d_2 : T_2$. By induction, $\Gamma$ **vis** $x$.

□

**Lemma 5.45** (VVC). *If* $\Gamma_1, !, \Gamma_2$ **vis** $x$*, then* $x \in \mathrm{dom}\ \Gamma_2$*.*

*Proof.* By inversion of (Vis-Var), $\Gamma_1, !, \Gamma_2 = \Gamma_3, x : T, \Gamma_4$, where $! \notin \Gamma_4$. Therefore $x$ must be after !, so $x \in \mathrm{dom}\ \Gamma_2$. □

**Lemma 5.46** (MLoc). *If* $\mathrm{F};\rho \vdash \langle t_0; \sigma; \rho; \Sigma\rangle : T_0$*, and* $y_1 \to d \in \Sigma$*, where* $d = \ldots_1 \{m(z, r) = t_3\} \ldots_2$*, then there is no* $v$ *for which* $t_3$ **tfree** $v$*.*

*Idea.* Method bodies cannot contain any t-free locations and references. ▽

*Proof idea.* Because of the use of ! in method definition typing, references and locations are not visible in the body and therefore cannot be t-free. ▽

*Proof.* By inversion of (CT-ObjH), $\mathrm{F}, y_1/s : R;\rho \vdash d : [y_1/s]R$. By induction on definition typing (DT-And) and (DT-Met), exists some $T_2$, $T_3$, $T_4$, such that $\Gamma_2;\rho \vdash t_3 : T_3$, where $\Gamma_2 = \mathrm{F}, !, r : T_4, z : T_2$. If $t_3$ **tfree** $v$, then by 5.44(VFV), $\Gamma_2$ **vis** $v$. By 5.45(VVC), $v \in \mathrm{dom}\ (r : T_4, z : T_2)$, which is a contradiction. □

**Lemma 5.47** (TFSub). *If* $[v_2/u]t$ $\mathbf{tfree}$ $v_1$*, then* $v_1 = v_2 \lor t$ $\mathbf{tfree}$ $v_1$*. If* $[v_2/u]d$ $\mathbf{tfree}$ $v_1$*, then* $v_1 = v_2 \lor d$ $\mathbf{tfree}$ $v_1$*.*

*Idea.* If $v_1$ is t-free in a term after substitution, then it was inserted by the substitution or it was t-free before substitution. ▽

*Proof idea.* If $v_1$ is not the newly substituted variable, then the same occurrence that makes it t-free after substitution also makes it t-free before substitution. ▽

*Proof.* Suppose that $v_1 \neq v_2$. Induction on $[v_2/u]t$ $\mathbf{tfree}$ $v_1$:

- Case (TF-Var): $[v_2/u]t = \mathsf{v}v_1$. By (EX-Var), $t = \mathsf{v}x$, and $v_1 = [v_2/u]x$. Because $v_1 \neq v_2$, then $u \neq x$, and $x = v_2$, so by (TF-Var), $\mathsf{v}x$ $\mathbf{tfree}$ $v_2$.
- Case (TF-Apply1): $[v_2/u]t = v_1.m\,x_2$. By (EX-Apply), $t = x_1.m\,x_3$, and $v_1 = [v_2/u]x_1$. Because $v_1 \neq v_2$, then $u \neq x_1$, and $x_1 = v_2$, so by (TF-Apply1), $x_1.m\,x_3$ $\mathbf{tfree}$ $v_2$.
- Case (TF-Apply2): $[v_2/u]t = x_1.m\,v_1$. By (EX-Apply), $t = x_3.m\,x_2$, and $v_1 = [v_2/u]x_2$. Because $v_1 \neq v_2$, then $u \neq x_2$, and $x_2 = v_2$, so by (TF-Apply2), $x_3.m\,x_2$ $\mathbf{tfree}$ $v_2$.
- Case (TF-Read): $[v_2/u]t = v_1.a$. By (EX-Read), $t = x_1.a$, and $v_1 = [v_2/u]x_1$. Because $v_1 \neq v_2$, then $u \neq x_1$, and $x_1 = v_2$, so by (TF-Read), $x_1.a$ $\mathbf{tfree}$ $v_2$.
- Case (TF-Write1): $[v_2/u]t = v_1.a := x_2$. By (EX-Write), $t = x_1.a := x_3$, and $v_1 = [v_2/u]x_1$. Because $v_1 \neq v_2$, then $u \neq x_1$, and $x_1 = v_2$, so by (TF-Write1), $x_1.a := x_3$ $\mathbf{tfree}$ $v_2$.
- Case (TF-Write2): $[v_2/u]t = x_1.a := v_1$. By (EX-Write), $t = x_3.a := x_2$, and $v_1 = [v_2/u]x_2$. Because $v_1 \neq v_2$, then $u \neq x_2$, and $x_2 = v_2$, so by (TF-Write2), $x_3.a := x_2$ $\mathbf{tfree}$ $v_2$.
- Case (TF-NewD): $[v_2/u]t = \mathsf{let}\ z = \nu(s : R_1)d_1\ \mathsf{in}\ t_1$. $d_1$ $\mathbf{tfree}$ $v_1$. By (EX-LetNew), $t = \mathsf{let}\ z = \nu(s : R_2)d_2\ \mathsf{in}\ t_2$, and $[v_2/u]d_2$ $\mathbf{tfree}$ $v_1$, where $d_1 = [v_2/u]d_2$. By induction, $d_2$ $\mathbf{tfree}$ $v_1$. By (TF-NewD), $\mathsf{let}\ z = \nu(s : R_2)d_2\ \mathsf{in}\ t_2$ $\mathbf{tfree}$ $v_1$.
- Case (TF-NewT): $[v_2/u]t = \mathsf{let}\ z = \nu(s : R_1)d_1\ \mathsf{in}\ t_1$. $d_1$ $\mathbf{tfree}$ $v_1$. By (EX-LetNew), $t = \mathsf{let}\ z = \nu(s : R_2)d_2\ \mathsf{in}\ t_2$, and $[v_2/u]t_2$ $\mathbf{tfree}$ $v_1$, where $t_1 = [v_2/u]t_2$. By induction, $t_2$ $\mathbf{tfree}$ $v_1$. By (TF-NewT), $\mathsf{let}\ z = \nu(s : R_2)d_2\ \mathsf{in}\ t_2$ $\mathbf{tfree}$ $v_1$.
- Case (TF-LetPush): $[v_2/u]t = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$. $t_1$ $\mathbf{tfree}$ $v_1$. By (EX-Let), $t = \mathsf{let}\ z = t_3\ \mathsf{in}\ t_4$, and $[v_2/u]t_3$ $\mathbf{tfree}$ $v_1$, where $t_1 = [v_2/u]t_3$. By induction, $d_2$ $\mathbf{tfree}$ $v_1$. By (TF-LetPush), $\mathsf{let}\ z = t_3\ \mathsf{in}\ t_4$ $\mathbf{tfree}$ $v_1$.
- Case (TF-LetPop): $[v_2/u]t = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$. $t_2$ $\mathbf{tfree}$ $v_1$. By (EX-Let), $t = \mathsf{let}\ z = t_3\ \mathsf{in}\ t_4$, and $[v_2/u]t_4$ $\mathbf{tfree}$ $v_1$, where $t_2 = [v_2/u]t_4$. By induction, $d_2$ $\mathbf{tfree}$ $v_1$. By (TF-LetPop), $\mathsf{let}\ z = t_3\ \mathsf{in}\ t_4$ $\mathbf{tfree}$ $v_1$.
- Case (TF-And1): $[v_2/u]d = d_1 \land d_2$. $d_1$ $\mathbf{tfree}$ $v_1$. By (DX-And), $d = d_3 \land d_4$, and $[v_2/u]d_3$ $\mathbf{tfree}$ $v_1$, where $d_1 = [v_2/u]d_3$. By induction, $d_3$ $\mathbf{tfree}$ $v_1$. By (TF-And1), $d_3 \land d_4$ $\mathbf{tfree}$ $v_1$.
- Case (TF-And2): $[v_2/u]d = d_1 \land d_2$. $d_2$ $\mathbf{tfree}$ $v_1$. By (DX-And), $d = d_3 \land d_4$, and $[v_2/u]d_4$ $\mathbf{tfree}$ $v_1$, where $d_2 = [v_2/u]d_4$. By induction, $d_4$ $\mathbf{tfree}$ $v_1$. By (TF-And2), $d_3 \land d_4$ $\mathbf{tfree}$ $v_1$.
- Case (TF-Fld): $[v_2/u]d = \{a = v_1\}$. By (DX-Fld), $d = \{a = x_1\}$, where $v_1 = [v_2/u]x_1$. Because $v_1 \neq v_2$, then $u \neq x_1$, and $x_1 = v_2$. By (TF-Fld), $\{a = x_1\}$ $\mathbf{tfree}$ $v_2$.
- Case (TF-Met): $[v_2/u]d = \{a(z, r) = t_1\}$. $t_1$ $\mathbf{tfree}$ $v_1$. By (DX-Met), $d = \{a(z, r) = t_2\}$, and $[v_2/u]t_2$ $\mathbf{tfree}$ $v_1$, where $t_1 = [v_2/u]t_2$. By induction, $t_2$ $\mathbf{tfree}$ $v_1$. By (TF-Met), $\{a(z, r) = t_2\}$ $\mathbf{tfree}$ $v_1$.

□

### 5.2.2 Precise typing lemmata

This section states properties of the precise typing relation defined in Section 4.3.

Because types in an inert context have a prescribed form, precise typing can only give variables a type of one of four forms.

**Lemma 5.48** (PrecForms). *If* $\mathrm{F} \vdash_! v : T_1$, *then either* $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}$ *or* $T_1 = \mu(s : R)$ *or* $T_1 = \{\mathsf{M}(r_0) : \bot..T_2\}$ *or* $[v/s]R = \ldots_1 T_1 \ldots_2$, *where* $\mathrm{F} = \mathrm{F}_1, v : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \mathrm{F}_2$.

*Proof.* Induction on $\mathrm{F} \vdash_! v : T_1$:

- Case (VT$_!$-Var): $\mathrm{F} = \mathrm{F}_1, v : T_1, \mathrm{F}_2$. By inertness of F, $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}$.
- Case (VT$_!$-Rec): $T_1 = [v/s_1]T_3$, where $\mathrm{F} \vdash_! v : \mu(s_1 : T_3)$. By induction, $s_1 = s$, and $T_3 = R$. By (TL-Refl), $[v/s]R = \ldots_1 T_1 \ldots_2$.
- Case (VT$_!$-And1): $\mathrm{F} \vdash_! v : T_1 \wedge T_3$. By induction, $T_1 = \mu(s : R)$, or $[v/s]R = \ldots_3 T_1 \wedge T_3 \ldots_4$. In the second case, there exist $\ldots_1, \ldots_2$, such that $[v/s]R = \ldots_1 T_1 \ldots_2$.
- Case (VT$_!$-And2): $\mathrm{F} \vdash_! v : T_3 \wedge T_1$. By induction, $T_1 = \{\mathsf{M}(r_0) : \bot..T_2\}$, or $[v/s]R = \ldots_3 T_3 \wedge T_1 \ldots_4$. In the second case, there exist $\ldots_1, \ldots_2$, such that $[v/s]R = \ldots_1 T_1 \ldots_2$.

□

**Lemma 5.49** (NoPrecTyp). $\mathrm{F} \nvdash_! v : \bot$, $\mathrm{F} \nvdash_! v : v_1.B(x)$, $\mathrm{F} \nvdash_! v : T_1 \vee T_2$, $\mathrm{F} \nvdash_! v : \mathsf{N}$, $\mathrm{F} \nvdash_! v : \top$, $\mathrm{F} \nvdash_! v : \{B(r) : T_1..T_2\} \wedge \{B(r) : T_3..T_4\}$.

*Proof idea.* By precise typing and structure of types in an inert context. ▽

*Proof.* Types in the inert context have the form $\mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T\}$, where $R$ is an intersection of types, which cannot be any of the types in this lemma. □

To simplify some proofs about precise typing, we show equivalence of precisse typing with a simplified version which derives the precise type in one step.

**Lemma 5.50** (PrecSim). *If* $\mathrm{F} \vdash_! v : \{B(r) : T_1..T_2\}$, *then either* $B = \mathsf{M}$, *and* $\mathrm{F} \vdash_{!2} v : \{\mathsf{M}(r) : T_1..T_2\}$ *or* $B \neq \mathsf{M}$, *and* $\mathrm{F} \vdash_{!1} v : \{B(r) : T_1..T_2\}$. *If* $\mathrm{F} \vdash_! v : \{m(z : T_1, r : T_3) : T_2\}$, *then* $\mathrm{F} \vdash_{!1} v : \{m(z : T_1, r : T_3) : T_2\}$. *If* $\mathrm{F} \vdash_! v : \{a : T_1..T_2\}$, *then* $\mathrm{F} \vdash_{!1} v : \{a : T_1..T_2\}$.

*Proof.*

- Type member: By 5.48(PrecForms), $\mathrm{F} = \mathrm{F}_1, v : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_4\}, \mathrm{F}_2$. If $B \neq \mathsf{M}$, then $[v/s]R = \ldots_1 \{B(r) : T_1..T_2\} \ldots_2$, then by (VT$_{!1}$-Var). Otherwise, by inertness of F, $\{B(r) : T_1..T_2\} = \{\mathsf{M}(r_0) : \bot..T_4\}$, then by (VT$_{!2}$-Var).
- Field member: By 5.48(PrecForms), $\mathrm{F} = \mathrm{F}_1, v : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_4\}, \mathrm{F}_2$, and $[v/s]R = \ldots_1 \{a : T_1..T_2\} \ldots_2$. By (VT$_{!1}$-Var).
- Method member: By 5.48(PrecForms), $\mathrm{F} = \mathrm{F}_1, v : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_4\}, \mathrm{F}_2$, and $[v/s]R = \ldots_1 \{m(z : T_1, r : T_3) : T_2\} \ldots_2$. By (VT$_{!1}$-Var).

□

**Lemma 5.51** (PrecSimInv). *If* $\mathrm{F} \vdash_{!1} v : T$, *then* $\mathrm{F} \vdash_! v : T$.

*Proof.* By inversion of (VT$_{!1}$-Var), $\mathrm{F} = \mathrm{F}_1, v : \mu(s : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \mathrm{F}_2$, and $[v/s]R_1 = \ldots_1 T \ldots_2$. By (VT$_!$-Var), $\mathrm{F} \vdash_! v : \mu(s : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}$. By (VT$_!$-And1), $\mathrm{F} \vdash_! v : \mu(s : R_1)$. By (VT$_!$-Rec), $\mathrm{F} \vdash_! v : [v/s]R_1$. By (VT$_!$-And1) and (VT$_!$-And2), $\mathrm{F} \vdash_! v : T$. □

For a type member in an object, the declaration type given by precise typing is uniquely determined (stated by 5.52(UPrecTyp)) and the bounds are tight or the lower bound is $\bot$ (stated by 5.53(SubPrecTyp)).

**Lemma 5.52** (UPrecTyp). *If* $\mathrm{F} \vdash_! v : \{B(r) : T_1..T_2\}$, *and* $\mathrm{F} \vdash_! v : \{B(r) : T_3..T_4\}$, *then* $T_1 = T_3$, *and* $T_2 = T_4$.

*Proof idea.* By inversion of simplified precise typing and by structure of types in an inert context ▽

*Proof.*

- If $B = \mathsf{M}$, then by 5.50(PrecSim), $\mathrm{F} \vdash_{!2} v : \{B(r) : T_1..T_2\}$, and $\mathrm{F} \vdash_{!2} v : \{B(r) : T_3..T_4\}$. By inversion of (VT$_{!2}$-Var), $\mathrm{F} = \mathrm{F}_1, v : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_5\}, \mathrm{F}_2$, and $\{\mathsf{M}(r_0) : \bot..T_5\} = \{B(r) : T_1..T_2\}$, and $\mathrm{F} = \mathrm{F}_3, v : \mu(s_2 : R_2) \wedge \{\mathsf{M}(r_0) : \bot..T_6\}, \mathrm{F}_4$, and $\{\mathsf{M}(r_0) : \bot..T_6\} = \{B(r) : T_3..T_4\}$. Because $v \notin \mathrm{dom}\ \mathrm{F}_2$, and $v \notin \mathrm{dom}\ \mathrm{F}_4$, we have $T_5 = T_6$, therefore $T_1 = T_3$, and $T_2 = T_4$.

- If $B \neq \mathsf{M}$, then by 5.50(PrecSim), $\mathrm{F} \vdash_{!1} v : \{B(r) : T_1..T_2\}$, and $\mathrm{F} \vdash_{!1} v : \{B(r) : T_3..T_4\}$. By inversion of (VT$_{!1}$-Var), $\mathrm{F} = \mathrm{F}_1, v : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_5\}, \mathrm{F}_2$, and $[v/s_1]R_1 = \ldots_1 \{B(r) : T_1..T_2\} \ldots_2$, and $\mathrm{F} = \mathrm{F}_3, v : \mu(s_2 : R_2) \wedge \{\mathsf{M}(r_0) : \bot..T_6\}, \mathrm{F}_4$, and $[v/s_2]R_2 = \ldots_3 \{B(r) : T_3..T_4\} \ldots_4$. Because $v \notin \mathrm{dom}\ \mathrm{F}_2$, and $v \notin \mathrm{dom}\ \mathrm{F}_4$, we have $R_1 = R_2$, and $s_1 = s_2$. Because member names in an inert context are unique, therefore $T_1 = T_3$, and $T_2 = T_4$.

□

**Lemma 5.53** (SubPrecTyp). *If* $\mathrm{F} \vdash_! v : \{B(r) : T_1..T_2\}$*, then either* $T_1 = T_2$ *or* $T_1 = \bot$*.*

*Idea.* In type member types given by precise typing, the lower bound either $\bot$ or the same as the upper bound ▽

*Proof idea.* In an record type, the bounds are either the same, or the lower bound is $\bot$. Substituting $s$ does not change that. ▽

*Proof.* If $B = \mathsf{M}$, then by 5.50(PrecSim), $\mathrm{F} \vdash_{!2} v : \{B(r) : T_1..T_2\}$. By inversion of (VT$_{!2}$-Var), $\mathrm{F} = \mathrm{F}_1, v : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_5\}, \mathrm{F}_2$, and $\{\mathsf{M}(r_0) : \bot..T_5\} = \{B(r) : T_1..T_2\}$, therefore $T_1 = \bot$. If $B \neq \mathsf{M}$, then by 5.50(PrecSim), $\mathrm{F} \vdash_{!1} v : \{B(r) : T_1..T_2\}$. By inversion of (VT$_{!1}$-Var), $\mathrm{F} = \mathrm{F}_1, v : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_5\}, \mathrm{F}_2$, and $[v/s]R_1 = \ldots_1 \{B(r) : T_1..T_2\} \ldots_2$. By inertness of F, $T_1 = T_2$, or $T_1 = \bot$. □

Because of the similarity of the types given to a location and a reference to the same object, the type declaration types given to these variables are equivalent.

Lemma 5.54(EqPrecTypL) states this for a reference and a location, when one of the types is known. Lemma 5.55(EqPrecTyp) states this for two general global variables, when one of the types is known. Lemma 5.56(EqPrecTypG) states this for two general global variables, when both of the types are known.

**Lemma 5.54** (EqPrecTypL). *If* $w \to y \in \rho$ *and* $\mathrm{F} \sim \rho$*, then*

- *If* $\mathrm{F} \vdash_! w : \{A(r) : T_1..T_2\}$*, then there exist* $T_3$*,* $T_4$*, such that* $\mathrm{F} \vdash_! y : \{A(r) : T_3..T_4\}$*, and* $\rho \vdash T_1 \approx T_3$*, and* $\rho \vdash T_2 \approx T_4$*.*
- *If* $\mathrm{F} \vdash_! y : \{A(r) : T_5..T_6\}$*, then there exist* $T_7$*,* $T_8$*, such that* $\mathrm{F} \vdash_! w : \{A(r) : T_7..T_8\}$*, and* $\rho \vdash T_5 \approx T_7$*, and* $\rho \vdash T_6 \approx T_8$*.*

*Idea.* The precise types of a type member as seen from a reference and as seen from a location exist if the other one exists, and they are equivalent. ▽

*Proof idea.* The bounds are obtained by taking the bounds from the heap type and substituting either $w$ or $y$ for $s$. ▽

*Proof.* By 5.50(PrecSim), $\mathrm{F} \vdash_{!1} w : \{A(r) : T_1..T_2\}$, and $\mathrm{F} \vdash_{!1} y : \{A(r) : T_5..T_6\}$. By inversion of (VT$_{!1}$-Var), $\mathrm{F} = \mathrm{F}_1, w : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\}, \mathrm{F}_2$, and $[w/s_1]R_1 = \ldots_1 \{A(r) : T_1..T_2\} \ldots_2$. By 5.16(ECorrInvY), $\mathrm{F} = \mathrm{F}_3, y : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_4$. Choose $T_3$, and $T_4$, such that $R_1 = \ldots_9 \{A(r) : T_9..T_{10}\} \ldots_{10}$, and $T_3 = [y/s_1]T_9$, and $T_4 = [y/s_1]T_{10}$, therefore $[y/s_1]R_1 = \ldots_3 \{A(r) : T_3..T_4\} \ldots_4$. By inertness of F, $R_1$ **indep** $s_1$, therefore $T_9$ **indep** $s_1$, and $T_{10}$ **indep** $s_1$. By 5.67(IndepEq), $\rho \vdash T_1 \approx T_3$, and $\rho \vdash T_2 \approx T_4$. By (VT$_{!1}$-Var), $\mathrm{F} \vdash_{!1} y : \{A(r) : T_3..T_4\}$. By 5.51(PrecSimInv), $\mathrm{F} \vdash_! y : \{A(r) : T_3..T_4\}$. By inversion of (VT$_{!1}$-Var), $\mathrm{F} = \mathrm{F}_5, y : \mu(s_2 : R_2) \wedge \{\mathsf{M}(r_0) : \bot..T_{14}\}, \mathrm{F}_6$, and $[y/s_2]R_2 = \ldots_5 \{A(r) : T_5..T_6\} \ldots_6$. By 5.17(ECorrInvW), $\mathrm{F} = \mathrm{F}_7, w : \mu(s_2 : R_2) \wedge \{\mathsf{M}(r_0) : \bot..T_{15}\}, \mathrm{F}_8$. Choose $T_7$, and $T_8$, such that $R_2 = \ldots_{11} \{A(r) : T_{11}..T_{12}\} \ldots_{12}$, and $T_7 = [w/s_2]T_{11}$, and $T_8 = [w/s_2]T_{12}$, therefore $[w/s_1]R_1 = \ldots_7 \{A(r) : T_7..T_8\} \ldots_8$. By inertness of F, $R_2$ **indep** $s_2$, therefore $T_{11}$ **indep** $s_2$, and $T_{12}$ **indep** $s_2$. By 5.67(IndepEq), $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By (VT$_{!1}$-Var), $\mathrm{F} \vdash_{!1} w : \{A(r) : T_7..T_8\}$. By 5.51(PrecSimInv), $\mathrm{F} \vdash_! w : \{A(r) : T_7..T_8\}$. □

**Lemma 5.55** (EqPrecTyp). *If* $\rho \vdash v_1 \approx v_2$ *and* $\mathrm{F} \sim \rho$*, then*

- *If* $\mathrm{F} \vdash_! v_1 : \{A(r) : T_1..T_2\}$*, then there exist* $T_3$*,* $T_4$*, such that* $\mathrm{F} \vdash_! v_2 : \{A(r) : T_3..T_4\}$*, and* $\rho \vdash T_1 \approx T_3$*, and* $\rho \vdash T_2 \approx T_4$*.*
- *If* $\mathrm{F} \vdash_! v_2 : \{A(r) : T_5..T_6\}$*, then there exist* $T_7$*,* $T_8$*, such that* $\mathrm{F} \vdash_! v_1 : \{A(r) : T_7..T_8\}$*, and* $\rho \vdash T_5 \approx T_7$*, and* $\rho \vdash T_6 \approx T_8$*.*

*Idea.* The precise types of a type member as seen from two equivalent variables exist if the other one exists, and they are equivalent. ▽

*Proof idea.* By induction, 5.54(EqPrecTypL) and equivalence properties of $\vdash\approx$ ▽

*Proof.* Induction on $\rho \vdash v_1 \approx v_2$:

- Case (VE-RtoL): $v_1 \to v_2 \in \rho$. Because $\mathrm{F} \sim \rho$, therefore $v_1 = w$, and $v_2 = y$. By 5.54(EqPrecTypL).
- Case (VE-Refl): $v_1 = v_2$. By 5.52(UPrecTyp) and (TE-Refl).
- Case (VE-Symm): $\rho \vdash v_2 \approx v_1$. By induction.
- Case (VE-Trans): $\rho \vdash v_1 \approx v_3$, and $\rho \vdash v_3 \approx v_2$. By induction, exist $T_9$, $T_{10}$, such that $\mathrm{F} \vdash_! v_3 : \{A(r) : T_9..T_{10}\}$, and $\rho \vdash T_1 \approx T_9$, and $\rho \vdash T_2 \approx T_{10}$. By induction, exist $T_3$, $T_4$, such that $\mathrm{F} \vdash_! v_2 : \{A(r) : T_3..T_4\}$, and $\rho \vdash T_9 \approx T_3$, and $\rho \vdash T_{10} \approx T_4$. By 5.3(EqTrans). By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F} \vdash_! v_3 : \{A(r) : T_{11}..T_{12}\}$, and $\rho \vdash T_5 \approx T_{11}$, and $\rho \vdash T_6 \approx T_{12}$. By induction, exist $T_7$, $T_8$, such that $\mathrm{F} \vdash_! v_1 : \{A(r) : T_7..T_8\}$, and $\rho \vdash T_{11} \approx T_7$, and $\rho \vdash T_{12} \approx T_8$. By 5.3(EqTrans).

□

**Lemma 5.56** (EqPrecTypG). *If* $\rho \vdash v_1 \approx v_2$*, and* $\mathrm{F} \sim \rho$*, and* $\mathrm{F} \vdash_! v_1 : \{A(r) : T_1..T_2\}$*, and* $\mathrm{F} \vdash_! v_2 : \{A(r) : T_3..T_4\}$*, then* $\rho \vdash T_1 \approx T_3$*, and* $\rho \vdash T_2 \approx T_4$*.*

*Idea.* The precise types of a type member as seen from two equivalent variables are equivalent. ▽

*Proof idea.* By 5.55(EqPrecTyp) and uniqueness of precise types ▽

*Proof.* By 5.55(EqPrecTyp), exist $T_5$, $T_6$, such that $\mathrm{F} \vdash_! v_2 : \{A(r) : T_5..T_6\}$, and $\rho \vdash T_1 \approx T_5$, and $\rho \vdash T_2 \approx T_6$. By 5.52(UPrecTyp), $T_3 = T_5, T_4 = T_6$. □

The following lemmata 5.57(CtxM) and 5.58(CtxF) show how from a field or method declaration type given by precise typing, we can see that the record type in the inter typing context contains a corresponding declaration. This is one step in showing that the object actually contains the member.

**Lemma 5.57** (CtxM). *If* $\mathrm{F} \vdash_! y_1 : \{m(z : T_6, r : T_8) : T_7\}$*, then* $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : \ldots_3 \{m(z : T_9, r : T_{11}) : T_{10}\} \ldots_4) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$*, and* $y_1 \notin \mathrm{dom}\ \mathrm{F}_2$*, and* $T_6 = [y_1/s]T_9$ *and* $T_8 = [y_1/s]T_{11}$ *and* $T_7 = [y_1/s]T_{10}$*.*

*Idea.* If a location has a precise method type, then the method type is a part of the location type in the context. ▽

*Proof.* By 5.50(PrecSim), $\mathrm{F} \vdash_{!1} y_1 : \{m(z : T_6, r : T_8) : T_7\}$. By inversion of (VT$_{!1}$-Var), we have $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T\}, \mathrm{F}_2$, and $[v/s]R = \ldots_1 \{m(z : T_6, r : T_8) : T_7\} \ldots_2$, and $y_1 \notin \mathrm{dom}\ \mathrm{F}_2$, therefore exist $T_9$, $T_{11}$, $T_{10}$, such that $R = \ldots_3 \{m(z : T_9, r : T_{11}) : T_{10}\} \ldots_4$, and $T_6 = [y_1/s]T_9$ and $T_8 = [y_1/s]T_{11}$ and $T_7 = [y_1/s]T_{10}$. By inertness of F, $T = \bot$. □

**Lemma 5.58** (CtxF). *If* $\mathrm{F} \vdash_! y_1 : \{a : T_9..T_8\}$*, then there exists* $T_5$*, such that* $[y_1/s]T_5 = T_8 = T_9$*, and* $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : \ldots_3 \{a : T_5..T_5\} \ldots_4) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$*, and* $y_1 \notin \mathrm{dom}\ \mathrm{F}_2$*.*

*Proof idea.* (Adapted from kDOT [2] Lemma 4.7.7 (page 46).) ▽

*Proof.* By 5.50(PrecSim), $\mathrm{F} \vdash_{!1} y_1 : \{a : T_9..T_8\}$. By inversion of (VT$_{!1}$-Var), we have $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T\}, \mathrm{F}_2$, and $[v/s]R = \ldots_1 \{a : T_9..T_8\} \ldots_2$, and $y_1 \notin \mathrm{dom}\ \mathrm{F}_2$, therefore exist $T_{10}$, $T_5$, such that $R = \ldots_3 \{a : T_{10}..T_5\} \ldots_4$, and $T_8 = [y_1/s]T_5$ and $T_9 = [y_1/s]T_{10}$. By inertness of F, $T = \bot$, and $T_{10} = T_5$. Because of determinism of substitution, $T_8 = T_9$. □

### 5.2.3 Invertible typing lemmata

This section states properties of the invertible typing relation defined in Section 4.7.

The types $\bot$ and $\mathsf{N}$ act only as lower bounds and there cannot be any objects that have these types. Lemma 5.59(NoInvTyp) shows that these types are never given by invertible typing.

**Lemma 5.59** (NoInvTyp). $\mathrm{F};\rho \nvdash_{\#\#} v : \bot$, $\mathrm{F};\rho \nvdash_{\#\#} v : \mathsf{N}$.

*Idea.* Types $\bot$ and $\mathsf{N}$ are never derived by invertible typing. ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-Var): By 5.49(NoPrecTyp).
- Other cases syntactically cannot derive $\bot$ or $\mathsf{N}$.

□

The following lemmata invert the rules of invertible typing. Note that unlike in DOT, the (VT$_{\#\#}$-Eq) rule requires using induction.

**Lemma 5.60** (InvT). *If* $\mathrm{F};\rho_1 \vdash_{\#\#} v : \{B(r) : T_1..T_2\}$*, then there exist* $T_5$*,* $T_4$*, such that* $\mathrm{F} \vdash_! v : \{B(r) : T_5..T_4\}$*, and* $\mathrm{F};\rho \vdash_{\#} T_1 <: T_5$*, and* $\mathrm{F};\rho \vdash_{\#} T_4 <: T_2$*.*

*Idea.* For invertible typing to a type member, there is a precise typing to a type member with tighter bounds. ▽

*Proof idea.* (Adapted from kDOT [2], page 49). ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-Typ): By induction and (ST$_{\#}$-Trans).
- Case (VT$_{\#\#}$-Eq): $\mathrm{F};\rho \vdash_{\#\#} v : T_{14}$, and $\rho \vdash \{B(r) : T_1..T_2\} \approx T_{14}$. By inversion of (TE-Typ), $T_{14} = \{B(r) : T_{11}..T_{12}\}$, and $\rho \vdash T_1 \approx T_{11}$, and $\rho \vdash T_2 \approx T_{12}$. By induction, $\mathrm{F} \vdash_! v : \{B(r) : T_5..T_4\}$, and $\mathrm{F};\rho \vdash_{\#} T_{11} <: T_5$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_{12}$. By (ST$_{\#}$-Eq), $\mathrm{F};\rho \vdash_{\#} T_1 <: T_{11}$, and $\mathrm{F};\rho \vdash_{\#} T_{12} <: T_2$. By (ST$_{\#}$-Trans), $\mathrm{F};\rho \vdash_{\#} T_1 <: T_5$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_2$.
- Case (VT$_{\#\#}$-Var): $\mathrm{F} \vdash_! v : \{B(r) : T_1..T_2\}$. Choose $T_5 = T_1$, and $T_4 = T_2$. By (ST$_{\#}$-Refl).

□

**Lemma 5.61** (InvF). *If* $\mathrm{F};\rho_1 \vdash_{\#\#} y_1 : \{a : T_4..T_3\}$*, then there exist* $T_8$*,* $T_9$*, such that* $\mathrm{F} \vdash_! y_1 : \{a : T_9..T_8\}$*, and* $\mathrm{F};\rho \vdash_{\#} T_4 <: T_9$*, and* $\mathrm{F};\rho \vdash_{\#} T_8 <: T_3$*.*

*Idea.* For invertible typing to a field member, there is a precise typing to a field member with tighter bounds. ▽

*Proof idea.* (Adapted from kDOT [2], page 49). ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-Fld): $\Gamma;\rho \vdash_{\#\#} y_1 : \{a : T_{11}..T_{12}\}$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_{11}$, and $\mathrm{F};\rho \vdash_{\#} T_{12} <: T_3$. By induction, $\mathrm{F} \vdash_! y_1 : \{a : T_9..T_8\}$, and $\mathrm{F};\rho \vdash_{\#} T_{11} <: T_9$, and $\mathrm{F};\rho \vdash_{\#} T_8 <: T_{12}$. By (ST$_{\#}$-Trans), $\mathrm{F};\rho \vdash_{\#} T_4 <: T_9$, and $\mathrm{F};\rho \vdash_{\#} T_8 <: T_3$.
- Case (VT$_{\#\#}$-Var): $\mathrm{F} \vdash_! y_1 : \{a : T_4..T_3\}$. Choose $T_9 = T_4$, and $T_8 = T_3$. By (ST$_{\#}$-Refl).
- Case (VT$_{\#\#}$-Eq): $\mathrm{F};\rho \vdash_{\#\#} y_1 : T_{14}$, and $\rho \vdash \{a : T_4..T_3\} \approx T_{14}$. By inversion of (TE-Fld), $T_{14} = \{a : T_{11}..T_{12}\}$, and $\rho \vdash T_4 \approx T_{11}$, and $\rho \vdash T_3 \approx T_{12}$. By induction, $\mathrm{F} \vdash_! y_1 : \{a : T_9..T_8\}$, and $\mathrm{F};\rho \vdash_{\#} T_{11} <: T_9$, and $\mathrm{F};\rho \vdash_{\#} T_8 <: T_{12}$. By (ST$_{\#}$-Eq), $\mathrm{F};\rho \vdash_{\#} T_4 <: T_{11}$, and $\mathrm{F};\rho \vdash_{\#} T_{12} <: T_3$. By (ST$_{\#}$-Trans), $\mathrm{F};\rho \vdash_{\#} T_4 <: T_9$, and $\mathrm{F};\rho \vdash_{\#} T_8 <: T_3$.

□

**Lemma 5.62** (InvM). *If* $\mathrm{F};\rho \vdash_{\#\#} y_1 : \{m(z : T_3, r : T_5) : T_4\}$*, then* $\mathrm{F} \vdash_! y_1 : \{m(z : T_6, r : T_8) : T_7\}$*, and* $\mathrm{F};\rho \vdash_{\#} T_3 <: T_6$*, and* $\mathrm{F}, z : T_3;\rho \vdash T_5 <: T_8$*, and* $\mathrm{F}, z : T_3;\rho \vdash T_7 <: T_4$*.*

*Idea.* If a location has an invertible method type, then it has a precise method type. ▽

*Proof idea.* (Adapted from kDOT [2], page 49). ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-Met): By induction and (ST$_\#$-Trans) on the result type and (ST-Trans) on parameter type and mutability.
- Case (VT$_{\#\#}$-Var): By (ST$_\#$-Refl) and (ST-Refl).
- Case (VT$_{\#\#}$-Eq): F;$\rho \vdash_{\#\#} y_1 : T_{14}$, and $\rho \vdash \{m(z : T_3, r : T_5) : T_4\} \approx T_{14}$. By inversion of (TE-Met), $T_{14} = \{m(z : T_{11}, r : T_{13}) : T_{12}\}$, and $\rho \vdash T_3 \approx T_{11}$, and $\rho \vdash T_5 \approx T_{13}$, and $\rho \vdash T_4 \approx T_{12}$. By induction, F $\vdash_! y_1 : \{m(z : T_6, r : T_8) : T_7\}$, and F;$\rho \vdash_\# T_{11} <: T_6$, and F;$\rho \vdash_\# T_{13} <: T_8$, and F;$\rho \vdash_\# T_7 <: T_{12}$. By (ST$_\#$-Eq), F;$\rho \vdash_\# T_3 <: T_{11}$, and F;$\rho \vdash_\# T_5 <: T_{13}$, and F;$\rho \vdash_\# T_{12} <: T_4$. By (ST$_\#$-Trans), F;$\rho \vdash_\# T_3 <: T_6$, and F;$\rho \vdash_\# T_5 <: T_8$, and F;$\rho \vdash_\# T_7 <: T_4$.

□

**Lemma 5.63** (InvAnd). *If* F;$\rho \vdash_{\#\#} v : T_1 \wedge T_2$, *then* F;$\rho \vdash_{\#\#} v : T_1$, *and* F;$\rho \vdash_{\#\#} v : T_2$.

*Idea.* If a global variable has an invertible intersection type, then it has both the types in the intersection. ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-AndI): F;$\rho \vdash_{\#\#} v : T_1$, and F;$\rho \vdash_{\#\#} v : T_2$.
- Case (VT$_{\#\#}$-Var): F $\vdash_! v : T_1 \wedge T_2$. By (VT$_!$-And1), F $\vdash_! v : T_1$. By (VT$_{\#\#}$-Var), F;$\rho \vdash_{\#\#} v : T_1$. By (VT$_!$-And2), F $\vdash_! v : T_2$. By (VT$_{\#\#}$-Var), F;$\rho \vdash_{\#\#} v : T_2$.
- Case (VT$_{\#\#}$-Eq): F;$\rho \vdash_{\#\#} v : T_3$, and $\rho \vdash T_3 \approx T_1 \wedge T_2$. By 5.4(TEInv), $T_3 = T_4 \wedge T_5$, and $\rho \vdash T_4 \approx T_1$, and $\rho \vdash T_5 \approx T_2$. By induction, F;$\rho \vdash_{\#\#} v : T_4$, and F;$\rho \vdash_{\#\#} v : T_5$. By (VT$_{\#\#}$-Eq), F;$\rho \vdash_{\#\#} v : T_1$, and F;$\rho \vdash_{\#\#} v : T_2$.

□

**Lemma 5.64** (InvOr). *If* F;$\rho \vdash_{\#\#} v : T_1 \vee T_2$, *then* F;$\rho \vdash_{\#\#} v : T_1$ *or* F;$\rho \vdash_{\#\#} v : T_2$.

*Idea.* If a global variable has an invertible union type, then it has at least one of the types in the union. ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-Or1): F;$\rho \vdash_{\#\#} v : T_1$.
- Case (VT$_{\#\#}$-Or2): F;$\rho \vdash_{\#\#} v : T_2$.
- Case (VT$_{\#\#}$-Var): Not possible by 5.49(NoPrecTyp).
- Case (VT$_{\#\#}$-Eq): F;$\rho \vdash_{\#\#} v : T_3$, and $\rho \vdash T_3 \approx T_1 \vee T_2$. By 5.4(TEInv), $T_3 = T_4 \vee T_5$, and $\rho \vdash T_4 \approx T_1$, and $\rho \vdash T_5 \approx T_2$. By induction, either F;$\rho \vdash_{\#\#} v : T_4$, or F;$\rho \vdash_{\#\#} v : T_5$. By (VT$_{\#\#}$-Eq), either F;$\rho \vdash_{\#\#} v : T_1$, or F;$\rho \vdash_{\#\#} v : T_2$.

□

**Lemma 5.65** (InvRec). *If* F;$\rho \vdash_{\#\#} v : \mu(s : T_1)$, *then* F;$\rho \vdash_{\#\#} v : [v/s]T_1$.

*Idea.* If a global variable has an invertible recursive type, then it has the type with the self variable replaced. ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-RecI): F;$\rho \vdash_{\#\#} v : [v/s]T_1$.
- Case (VT$_{\#\#}$-Var): F $\vdash_! v : \mu(s : T_1)$. By (VT$_!$-Rec), F $\vdash_! v : [v/s]T_1$. By (VT$_{\#\#}$-Var), F;$\rho \vdash_{\#\#} v : [v/s]T_1$.
- Case (VT$_{\#\#}$-Eq): F;$\rho \vdash_{\#\#} v : T_2$, and $\rho \vdash T_2 \approx \mu(s : T_1)$. By 5.4(TEInv), $T_2 = \mu(s : T_3)$, and $\rho \vdash T_3 \approx T_1$. By induction, F;$\rho \vdash_{\#\#} v : [v/s]T_3$. By 5.26(SubEq), $\rho \vdash [v/s]T_3 \approx [v/s]T_1$. By (VT$_{\#\#}$-Eq), F;$\rho \vdash_{\#\#} v : [v/s]T_1$.

□

**Lemma 5.66** (InvSel). *If* $\mathrm{F};\rho \vdash_{\#\#} v : v_1.B(x)$*, then* $\mathrm{F};\rho \vdash_{\#\#} v : [x/r]T_3$*, where* $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_3..T_4\}$ *or* $B \neq \mathsf{M}$*, and* $\mathrm{F} \vdash_{!} v_2 : \{B(r) : T_3..T_4\}$*, and* $\rho \vdash v_2 \approx v_1$*.*

*Idea.* If a global variable has an invertible selection type, then it has the type of its bound. ▽

*Proof.* Induction on invertible typing:

- Case (VT$_{\#\#}$-Sel): $\mathrm{F};\rho \vdash_{\#\#} v : [x/r]T_3$, where $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_3..T_4\}$.
- Case (VT$_{\#\#}$-Var): Not possible by 5.49(NoPrecTyp).
- Case (VT$_{\#\#}$-Eq): $\mathrm{F};\rho \vdash_{\#\#} v : T_2$, and $\rho \vdash T_2 \approx v_1.B(x)$. By 5.4(TEInv), $T_2 = v_2.B(x)$, and $\rho \vdash v_2 \approx v_1$, and $B \neq \mathsf{M}$. By induction, $\mathrm{F};\rho \vdash_{\#\#} v : [x/r]T_3$, where $\mathrm{F} \vdash_{!} v_3 : \{B(r) : T_3..T_4\}$, and $\rho \vdash v_3 \approx v_2$. By 5.3(EqTrans), $\rho \vdash v_3 \approx v_1$.

□

### 5.2.4 Dereference lemmata

This section contains lemmata about deriving typing relations involving locations ($y$) from typing relations involving the corresponding references ($w$, when $w \to y \in \rho$).

**Lemma 5.67** (IndepEq). *If $T$ **indep** $s$, and $w \to y \in \rho$, then $\rho \vdash [w/s]T \approx [y/s]T$.*

*Idea.* If a type is independent, then $w$ and $y$ are interchangeable. ▽

*Proof.* Induction on type independence **indep** :

- Cases (TI-Top), (TI-Bot), (TI-N): $T = \top$, or $T = \bot$, or $T = \mathsf{N}$. In all these cases, $[w/s]T = [y/s]T$. By (TE-Refl).
- Case (TI-And): $T = T_1 \wedge T_2$. By induction, $\rho \vdash [w/s]T_1 \approx [y/s]T_1$, and $\rho \vdash [w/s]T_2 \approx [y/s]T_2$. By (TE-And).
- Case (TI-Or): $T = T_1 \vee T_2$. By induction, $\rho \vdash [w/s]T_1 \approx [y/s]T_1$, and $\rho \vdash [w/s]T_2 \approx [y/s]T_2$. By (TE-Or).
- Case (TI-SelM): $T = x_1.\mathsf{M}(x_2)$, where $x_1 \neq s$, and $x_2 \neq s$. $[w/s]T = [y/s]T$. By (TE-Refl).
- Case (TI-SelA): $T = x_1.A(x_2)$. $x_2 \neq s$. If $x_1 = s$, then by (VX-VarE), $[w/s]x_1 = w$, and $[y/s]x_1 = y$. By (VE-RtoL), $\rho \vdash w \approx y$ and (TE-Sel), $\rho \vdash w.A(x_2) \approx y.A(x_2)$. Otherwise, $x_1 \neq s$, $[w/s]T = [y/s]T$. By (TE-Refl).
- Case (TI-Rec): $T = \mu(s_1 : T_1)$. $T_1$ **indep** $s$. By induction, $\rho \vdash [w/s]T_1 \approx [y/s]T_1$. By (TE-Rec), $\rho \vdash \mu(s_1 : [w/s]T_1) \approx \mu(s_1 : [y/s]T_1)$.
- Case (TI-Fld): $T = \{a : T_1..T_2\}$. $T_1$ **indep** $s$. $T_2$ **indep** $s$. By induction, $\rho \vdash [w/s]T_1 \approx [y/s]T_1$, and $\rho \vdash [w/s]T_2 \approx [y/s]T_2$. By (TE-Fld), $\rho \vdash \{a : [w/s]T_1..[w/s]T_2\} \approx \{a : [y/s]T_1..[y/s]T_2\}$.
- Case (TI-Met): $T = \{m(z : T_1, r : T_3) : T_2\}$. $T_1$ **indep** $s$. $T_2$ **indep** $s$. $T_3$ **indep** $s$. By induction, $\rho \vdash [w/s]T_1 \approx [y/s]T_1$, and $\rho \vdash [w/s]T_2 \approx [y/s]T_2$, and $\rho \vdash [w/s]T_3 \approx [y/s]T_3$. By (TE-Met), $\rho \vdash \{m(z : [w/s]T_1, r : [w/s]T_3) : [w/s]T_2\} \approx \{m(z : [y/s]T_1, r : [y/s]T_3) : [y/s]T_2\}$.
- Case (TI-Typ): $T = \{B(r) : T_1..T_2\}$. $T_1$ **indep** $s$. $T_2$ **indep** $s$. By induction, $\rho \vdash [w/s]T_1 \approx [y/s]T_1$, and $\rho \vdash [w/s]T_2 \approx [y/s]T_2$. By (TE-Typ), $\rho \vdash \{B(r) : [w/s]T_1..[w/s]T_2\} \approx \{B(r) : [y/s]T_1..[y/s]T_2\}$.

□

**Lemma 5.68** (DerefT). *If $\Gamma;\rho \vdash w : T_1$, and $w \to y \in \rho$, and $\Gamma \sim \rho$, then $\Gamma;\rho \vdash y : T_1$.*

*Idea.* $y$ has all the types that a corresponding $w$ has. ▽

*Proof idea.* Induction on variable typing, using type equivalence to handle recursive types. ▽

*Proof.* Induction on variable typing:

- Case (VT-Var): $\Gamma = \Gamma_1, w : T_1, \Gamma_2$. By 5.16(ECorrInvY), $T_1 = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}$, and $\Gamma_1 = \Gamma_3, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \Gamma_4$. By (ST-Refl) and (ST-Bot) and 5.18(AndSub), $\Gamma; \rho \vdash \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: T_1$. By (VT-Var), $\Gamma;\rho \vdash y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$ and (VT-Sub), $\Gamma;\rho \vdash y : T_1$.
- Case (VT-RecI): $\Gamma;\rho \vdash w : [w/s]T_2$. $T_2$ **indep** $s$, where $T_1 = \mu(s : T_2)$. By induction, $\Gamma;\rho \vdash y : [w/s]T_2$. By 5.67(IndepEq), $\rho \vdash [w/s]T_2 \approx [y/s]T_2$. By (ST-Eq), $\Gamma;\rho \vdash [w/s]T_2 <: [y/s]T_2$. By (VT-Sub), $\Gamma;\rho \vdash y : [y/s]T_2$. By (VT-RecI), $\Gamma;\rho \vdash y : T_2$.
- Case (VT-RecE): $\Gamma;\rho \vdash w : \mu(s : T_2)$, where $T_1 = [w/s]T_2$, and $T_2$ **indep** $s$. By induction, $\Gamma; \rho \vdash y : \mu(s : T_2)$. By (VT-RecE), $\Gamma;\rho \vdash y : [y/s]T_2$. By 5.67(IndepEq), $\rho \vdash [w/s]T_2 \approx [y/s]T_2$. By 5.2(EqSymm), $\rho \vdash [y/s]T_2 \approx [w/s]T_2$. By (ST-Eq), $\Gamma;\rho \vdash [y/s]T_2 <: [w/s]T_2$. By (VT-Sub), $\Gamma; \rho \vdash y : [w/s]T_2$.
- Case (VT-AndI): $\Gamma;\rho \vdash w : T_2$, and $\Gamma;\rho \vdash w : T_3$, where $T_1 = T_2 \wedge T_3$. By induction, $\Gamma;\rho \vdash y : T_2$, and $\Gamma;\rho \vdash y : T_3$. By (VT-AndI), $\Gamma;\rho \vdash y : T_2 \wedge T_3$.
- Case (VT-MutTop): $T_1 = \{\mathsf{M}(r_0) : \bot..\top\}$. By (VT-MutTop).
- Case (VT-Sub): $\Gamma;\rho \vdash w : T_2$, where $\Gamma;\rho \vdash T_2 <: T_1$. By induction, $\Gamma;\rho \vdash y : T_2$. By (VT-Sub), $\Gamma; \rho \vdash y : T_1$.

□

The following lemmata show that replacing references by location preserves definition typing, and in the opposite direction that before the replacement, the reference must have been referring to the same object.

**Lemma 5.69** (DeD). *If* $\mathrm{F}, s : T_2;\rho \vdash d : T_1$*, and* $\mathrm{F} \sim \rho$*, then* $\mathrm{F}, s : T_2;\rho \vdash [\rho]d : T_1$.

*Idea.* Changing all references in an object definition to locations preserves its type. ▽

*Proof idea.* Induction on definition typing. Only fields are affected. ▽

*Proof.* Induction on $\mathrm{F}, s : T_2;\rho \vdash d : T_1$:

- Case (DT-Typ): $d = \{A(r) = T\}$. By (DU-Typ), $[\rho]\{A(r) = T\} = \{A(r) = T\}$. Directly by (DT-Typ).
- Case (DT-TypB): $d = \{A(r) = T\}$. By (DU-Typ), $[\rho]\{A(r) = T\} = \{A(r) = T\}$. Directly by (DT-TypB).
- Case (DT-Fld): $d = \{a = x\}$. $T_1 = \{a : T_3..T_3\}$. $\mathrm{F}, s : T_2;\rho \vdash x : T_3$. $\mathrm{F}, s : T_2$ **vis** $x$. $T_3$ **indep** $s$. If $x \in \mathrm{dom}\ \rho$, then $x = w$, where $w \to y \in \rho$, and $[\rho]x = y$. By 5.7(WknE), $\mathrm{F}, s : T_2 \sim \rho$. By 5.68(DerefT), $\mathrm{F}, s : T_2;\rho \vdash x : T_3$. By inertness of F, F **vis** $y$. By (DT-Fld), $\mathrm{F}, s : T_2;\rho \vdash \{a = y\} : T_1$. Otherwise, $x \notin \mathrm{dom}\ \rho$. By (DU-VarN), $[\rho]x = x$. By (DU-Fld), $[\rho]d = d$.
- Case (DT-And): $d = d_1 \wedge d_2$. $T_1 = T_3 \wedge T_4$. $\mathrm{F}, s : T_2;\rho \vdash d_1 : T_3$. $\mathrm{F}, s : T_2;\rho \vdash d_2 : T_4$. By induction, $\mathrm{F}, s : T_2;\rho \vdash [\rho]d_1 : T_3$, $\mathrm{F}, s : T_2;\rho \vdash [\rho]d_2 : T_4$. By (DU-And), $[\rho]d = [\rho]d_1 \wedge [\rho]d_2$. By (DT-And).
- Case (DT-Met): $d = \{m(z, r) = t\}$. By (DU-Met), $[\rho]\{m(z, r) = t\} = \{m(z, r) = t\}$. Directly by (DT-Met).

□

**Lemma 5.70** (DeInv). *If* $[\rho]d = \ldots_1 \{a = y\} \ldots_2$*, then either* $d = \ldots_3 \{a = x\} \ldots_4$*, where* $x \notin \mathrm{dom}\ \rho$ *or* $d = \ldots_3 \{a = v\} \ldots_4$*, where* $v \to y \in \rho$.

*Proof.* Induction on $[\rho]d = \ldots_1 \{a = y\} \ldots_2$:

- Case (DL-Refl): $[\rho]d = \{a = y\}$. By inversion of (DU-Fld), $d = \{a = x\}$, where $[\rho]x = y$. By inversion: Subcase (DU-Var): $x = w$, and $w \to y \in \rho$. Subcase (DU-VarN): $x \notin \mathrm{dom}\ \rho$.
- Cases (DL-And1), (DL-And2): By inversion of (DU-And), and by induction and (DL-And1) or by (DL-And2).

□

### 5.2.5 Typing equivalence lemmata

This section contains lemmata establishing equivalence of typing relations (normal, tight and invertible) in an inert context. The main lemma 5.77(VTEq) states that in an inert context, normal typing implies invertible typing. Typing equivalence lemmata and their proofs are adapted from kDOT [2].

The lemma 5.71(SubRTight) is a variant of 5.33(SubR), but for tight typing.

**Lemma 5.71** (SubRTight). *If* $\mathrm{F};\rho \vdash_{\#} T_3 <: T_1$*, then* $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_1$.

*Proof idea.* Substitution on tight subtyping. $r$ cannot be in the context, so it cannot be used in selection rules. ▽

*Proof.* We know that $r \notin \mathrm{F}$. Induction on $\mathrm{F};\rho \vdash_{\#} T_3 <: T_1$:

- Case (ST$_{\#}$-Top): $T_1 = \top$. Directly by (ST$_{\#}$-Top) and (TX-Top).
- Case (ST$_{\#}$-Bot): $T_3 = \bot$. Directly by (ST$_{\#}$-Bot) and (TX-Bot).
- Case (ST$_{\#}$-Refl): $T_3 = T_1$. Directly by (ST$_{\#}$-Refl).
- Case (ST$_{\#}$-And1): $T_3 = T_1 \wedge T_4$. By (ST$_{\#}$-And1), $\mathrm{F};\rho \vdash_{\#} [x/r]T_4 \wedge [x/r]T_1 <: [x/r]T_1$. By (TX-And).
- Case (ST$_{\#}$-And2): $T_3 = T_4 \wedge T_1$. By (ST$_{\#}$-And2), $\mathrm{F};\rho \vdash_{\#} [x/r]T_4 \wedge [x/r]T_1 <: [x/r]T_1$. By (TX-And).
- Case (ST$_{\#}$-And): $T_1 = T_4 \wedge T_5$, and $\mathrm{F};\rho \vdash_{\#} T_3 <: T_4$, and $\mathrm{F};\rho \vdash_{\#} T_3 <: T_5$. By induction on subtyping, $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_4$, $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_5$. By (ST$_{\#}$-And), $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_4 \wedge [x/r]T_5$. By (TX-And).
- Case (ST$_{\#}$-Or1): $T_1 = T_3 \vee T_4$. By (ST$_{\#}$-Or1), $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_3 \vee [x/r]T_4$. By (TX-Or).
- Case (ST$_{\#}$-Or2): $T_1 = T_4 \vee T_3$. By (ST$_{\#}$-Or2), $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_4 \vee [x/r]T_3$. By (TX-Or).
- Case (ST$_{\#}$-Or): $T_3 = T_4 \vee T_5$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_1$, and $\mathrm{F};\rho \vdash_{\#} T_5 <: T_1$. By induction on subtyping, $\mathrm{F};\rho \vdash_{\#} [x/r]T_4 <: [x/r]T_1$, $\mathrm{F};\rho \vdash_{\#} [x/r]T_5 <: [x/r]T_1$. By (ST$_{\#}$-Or), $\mathrm{F};\rho \vdash_{\#} [x/r]T_4 \vee [x/r]T_5 <: [x/r]T_1$. By (TX-Or).
- Case (ST$_{\#}$-Trans): $\mathrm{F};\rho \vdash_{\#} T_3 <: T_4$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_1$.

  By induction on subtyping, $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_4$, and $\mathrm{F};\rho \vdash_{\#} [x/r]T_4 <: [x/r]T_1$. By (ST$_{\#}$-Trans), $\mathrm{F};\rho \vdash_{\#} [x/r]T_3 <: [x/r]T_1$.
- Case (ST$_{\#}$-TypAnd): $T_3 = \{B(r_2) : T_4..T_5\} \wedge \{B(r_2) : T_6..T_7\}$, and $T_1 = \{B(r_2) : T_4 \vee T_6..T_5 \wedge T_7\}$. By (ST$_{\#}$-TypAnd) and (TX-And) and (TX-Or) and (TX-Typ).
- Case (ST$_{\#}$-Dist): $T_3 = T_4 \wedge (T_5 \vee T_6)$. $T_1 = (T_4 \wedge T_5) \vee (T_4 \wedge T_6)$. By (ST$_{\#}$-Dist) and (TX-Or) and (TX-And).
- Case (ST$_{\#}$-Typ): $T_3 = \{B(r_2) : T_4..T_5\}$, and $T_1 = \{B(r_2) : T_6..T_7\}$, where $\mathrm{F};\rho \vdash_{\#} T_6 <: T_4$, and $\mathrm{F};\rho \vdash_{\#} T_5 <: T_7$. Using alpha-equivalence, assume that $r$, $x$ are disjoint from $r_2$.

  By induction on subtyping, $\mathrm{F};\rho \vdash_{\#} [x/r]T_6 <: [x/r]T_4$, and $\mathrm{F};\rho \vdash_{\#} [x/r]T_5 <: [x/r]T_7$. By (ST$_{\#}$-Typ) and (TX-Typ).
- Case (ST$_{\#}$-Fld): $T_3 = \{a : T_4..T_5\}$, and $T_1 = \{a : T_6..T_7\}$, where $\mathrm{F};\rho \vdash_{\#} T_6 <: T_4$, and $\mathrm{F};\rho \vdash_{\#} T_5 <: T_7$.

  By induction on subtyping, $\mathrm{F};\rho \vdash_{\#} [x/r]T_6 <: [x/r]T_4$, and $\mathrm{F};\rho \vdash_{\#} [x/r]T_5 <: [x/r]T_7$. By (ST$_{\#}$-Fld) and (TX-Fld).
- Case (ST$_{\#}$-Met): $T_3 = \{m(z : T_4, r_2 : T_6) : T_5\}$, and $T_1 = \{m(z : T_7, r_2 : T_9) : T_8\}$, where $\mathrm{F};\rho \vdash_{\#} T_7 <: T_4$, and $\mathrm{F}, z : T_7;\rho \vdash T_9 <: T_6$, and $\mathrm{F}, z : T_7, r_2 : T_9;\rho \vdash T_5 <: T_8$. Using alpha-equivalence, assume that $r$, $x$ are disjoint from $r_2$ and $z$.

  By induction on subtyping, $\mathrm{F};\rho \vdash_{\#} [x/r]T_7 <: [x/r]T_4$. By 5.33(SubR), $\mathrm{F}, z : [x/r]T_7;\rho \vdash [x/r]T_9 <: [x/r]T_6$, and $\mathrm{F}, z : [x/r]T_7, r_2 : [x/r]T_9;\rho \vdash [x/r]T_5 <: [x/r]T_8$. By (ST$_{\#}$-Met) and (TX-Met).
- Case (ST$_{\#}$-N-M): $T_3 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_1 = \bot$. By (ST$_{\#}$-N-M) and (TX-Bot) and (TX-Typ) and (TX-N) and (TX-And).
- Case (ST$_{\#}$-N-Rec): $T_3 = \mathsf{N}$, and $T_1 = \mu(s : T_4)$. Using alpha-equivalence, assume that $r$, $x$ are disjoint from $s$. By (ST$_{\#}$-N-Rec) and (TX-Rec) and (TX-N).
- Case (ST$_{\#}$-N-Fld): $T_3 = \mathsf{N}$, and $T_1 = \{a : T_6..T_7\}$. By (ST$_{\#}$-N-Fld) and (TX-Fld) and (TX-N).

- Case (ST$_{\#}$-N-Met): $T_3 = \mathsf{N}$, and $T_1 = \{m(z : T_7, r_2 : T_9) : T_8\}$. Using alpha-equivalence, assume that $r$, $x$ are disjoint from $r_2$ and $z$. By (ST$_{\#}$-N-Met) and (TX-Met) and (TX-N).
- Case (ST$_{\#}$-N-Typ): $T_3 = \mathsf{N}$, and $T_1 = \{B(r_2) : T_6..T_7\}$. Using alpha-equivalence, assume that $r$, $x$ are disjoint from $r_2$. By (ST$_{\#}$-N-Typ) and (TX-Typ) and (TX-N).
- Case (ST$_{\#}$-Eq): $\rho \vdash T_3 \approx T_1$. By 5.26(SubEq), $\rho \vdash [x/r]T_3 \approx [x/r]T_1$. By (ST$_{\#}$-Eq).
- Case (ST$_{\#}$-SelL): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r_2) : T_4..T_5\}$, and $T_3 = [x_2/r_2]T_4$. Using alpha-equivalence, assume that $r \notin T_4$ and that $r_2$ is distinct from $r$ and $x_2$. By (ST$_{\#}$-SelL), F; $\rho \vdash_{\#} v_1.B([x/r]x_2) <: [[x/r]x_2/r_2]T_4$. By (VX-VarN), $[x/r]v_1 = v_1$. By 5.21(SubSwap) and (TX-Sel).
- Case (ST$_{\#}$-SelU): $T_3 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r_2) : T_4..T_5\}$, and $T_1 = [x_2/r_2]T_5$. Using alpha-equivalence, assume that $r \notin T_5$ and that $r_2$ is distinct from $r$ and $x_2$. By (ST$_{\#}$-SelU), F; $\rho \vdash_{\#} [[x/r]x_2/r_2]T_5 <: v_1.B([x/r]x_2)$. By (VX-VarN), $[x/r]v_1 = v_1$. By 5.21(SubSwap) and (TX-Sel).

□

The following lemmata follow the proof of soundness of [4].

The lemma 5.72(ClInv) shows that invertible typing is closed under tight subtyping. The proof is adapted from the Coq proof of [4].

**Lemma 5.72** (ClInv). *If* F;$\rho \vdash_{\#\#} v : T_1$, *and* F;$\rho \vdash_{\#} T_1 <: T_2$, *where* F $\sim \rho$, *then* F;$\rho \vdash_{\#\#} v : T_2$.

*Proof.* Induction on tight subtyping:

- Case (ST$_{\#}$-Top): $T_2 = \top$. By (VT$_{\#\#}$-Top), F;$\rho \vdash_{\#\#} v : \top$.
- Case (ST$_{\#}$-Bot): $T_1 = \bot$. Not possible by 5.59(NoInvTyp).
- Case (ST$_{\#}$-Refl): $T_1 = T_2$. By the premise.
- Cases (ST$_{\#}$-N-Rec), (ST$_{\#}$-N-Fld), (ST$_{\#}$-N-Met), (ST$_{\#}$-N-Typ): $T_1 = \mathsf{N}$. Not possible by 5.59(NoInvTyp).
- Case (ST$_{\#}$-N-M): $T_1 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.63(InvAnd), F;$\rho \vdash_{\#\#} v : \mathsf{N}$. Not possible by 5.59(NoInvTyp).
- Case (ST$_{\#}$-And1): $T_1 = T_2 \wedge T_3$. By 5.63(InvAnd), F;$\rho \vdash_{\#\#} v : T_2$.
- Case (ST$_{\#}$-And2): $T_1 = T_3 \wedge T_2$. By 5.63(InvAnd), F;$\rho \vdash_{\#\#} v : T_2$.
- Case (ST$_{\#}$-And): $T_2 = T_3 \wedge T_4$, where F;$\rho \vdash_{\#} T_1 <: T_3$, and F;$\rho \vdash_{\#} T_1 <: T_4$. By induction, F; $\rho \vdash_{\#\#} v : T_3$, and F;$\rho \vdash_{\#\#} v : T_4$. By (VT$_{\#\#}$-AndI), F;$\rho \vdash_{\#\#} v : T_3 \wedge T_4$.
- Case (ST$_{\#}$-Or1): $T_2 = T_1 \vee T_3$. By (VT$_{\#\#}$-Or1).
- Case (ST$_{\#}$-Or2): $T_2 = T_3 \vee T_1$. By (VT$_{\#\#}$-Or2).
- Case (ST$_{\#}$-Or): $T_1 = T_3 \vee T_4$, where F;$\rho \vdash_{\#} T_3 <: T_2$, and F;$\rho \vdash_{\#} T_4 <: T_2$. By 5.64(InvOr), F; $\rho \vdash_{\#\#} v : T_3$, or F;$\rho \vdash_{\#\#} v : T_4$. By induction, F;$\rho \vdash_{\#\#} v : T_2$.
- Case (ST$_{\#}$-Trans): F;$\rho \vdash_{\#} T_1 <: T_3$, and F;$\rho \vdash_{\#} T_3 <: T_2$. By induction, F;$\rho \vdash_{\#\#} v : T_3$. By induction, F;$\rho \vdash_{\#\#} v : T_2$.
- Case (ST$_{\#}$-SelL): $T_2 = v_2.B(x_1)$, and $T_1 = [x_1/r]T_3$, where $\mathrm{F} \vdash_! v_2 : \{B(r) : T_3..T_4\}$. By (VT$_{\#\#}$-Sel), F;$\rho \vdash_{\#\#} v : v_2.B(r)$.
- Case (ST$_{\#}$-SelU): $T_1 = v_2.B(x_1)$, and $T_2 = [x_1/r]T_4$, where $\mathrm{F} \vdash_! v_2 : \{B(r) : T_3..T_4\}$. By 5.66(InvSel), $\mathrm{F} \vdash_! v_2 : \{B(r) : T_5..T_6\}$, and F;$\rho \vdash_{\#\#} v : [x_1/r]T_5$, or $B \neq \mathsf{M}$, and $\mathrm{F} \vdash_! v_3 : \{B(r) : T_5..T_6\}$, and F;$\rho \vdash_{\#\#} v : [x_1/r]T_5$, and $\rho \vdash v_3 \approx v_2$.
  - If $B = \mathsf{M}$, then $\mathrm{F} \vdash_! v_2 : \{B(r) : T_5..T_6\}$, and F;$\rho \vdash_{\#\#} v : [x_1/r]T_5$. By 5.52(UPrecTyp), $T_5 = T_3$, and $T_6 = T_4$, so F;$\rho \vdash_{\#\#} v : [x_1/r]T_3$. By 5.53(SubPrecTyp), either $T_3 = T_4$, or $T_3 = \bot$. By 5.59(NoInvTyp), $T_3 \neq \bot$, so $T_3 = T_4$, and F;$\rho \vdash_{\#\#} v : [x_1/r]T_4$, so F;$\rho \vdash_{\#\#} v : T_2$.
  - If $B \neq \mathsf{M}$, then $\mathrm{F} \vdash_! v_3 : \{B(r) : T_5..T_6\}$, and F;$\rho \vdash_{\#\#} v : [x_1/r]T_5$, and $\rho \vdash v_3 \approx v_2$. By 5.53(SubPrecTyp), either $T_5 = T_6$, or $T_5 = \bot$. By 5.59(NoInvTyp), $T_5 \neq \bot$, so $T_5 = T_6$, so F; $\rho \vdash_{\#\#} v : [x_1/r]T_6$. By 5.56(EqPrecTypG) and 5.2(EqSymm), $\rho \vdash T_6 \approx T_4$. By 5.26(SubEq), $\rho \vdash [x_1/r]T_6 \approx [x_1/r]T_4$. By (VT$_{\#\#}$-Eq), F;$\rho \vdash_{\#\#} v : [x_1/r]T_4$, so F;$\rho \vdash_{\#\#} v : T_2$.
- Case (ST$_{\#}$-Typ): By (VT$_{\#\#}$-Typ).

- Case (ST$_\#$-TypAnd): $T_1 = \{B(r) : T_3..T_4\} \wedge \{B(r) : T_5..T_6\}$. $T_2 = \{B(r) : T_3 \vee T_5..T_4 \wedge T_6\}$. By 5.63(InvAnd). $\mathrm{F};\rho \vdash_{\#\#} v : \{B(r) : T_3..T_4\}$, and $\mathrm{F};\rho \vdash_{\#\#} v : \{B(r) : T_5..T_6\}$. By 5.60(InvT) and 5.52(UPrecTyp), exist $T_7$, $T_8$, such that $\mathrm{F} \vdash_{!} v : \{B(r) : T_7..T_8\}$, and $\mathrm{F};\rho \vdash_{\#} T_3 <: T_7$, and $\mathrm{F};\rho \vdash_{\#} T_5 <: T_7$, and $\mathrm{F};\rho \vdash_{\#} T_8 <: T_4$, and $\mathrm{F};\rho \vdash_{\#} T_8 <: T_6$. By (ST$_\#$-And), $\mathrm{F};\rho \vdash_{\#} T_8 <: T_4 \wedge T_6$. By (ST$_\#$-Or), $\mathrm{F};\rho \vdash_{\#} T_3 \vee T_5 <: T_7$. By (ST$_\#$-Typ), $\mathrm{F};\rho \vdash_{\#} \{B(r) : T_7..T_8\} <: \{B(r) : T_3 \vee T_5..T_4 \wedge T_6\}$. By (VT$_{\#\#}$-Var), $\mathrm{F} \vdash_{!} v : \{B(r) : T_7..T_8\}$. By (VT$_{\#\#}$-Typ), $\mathrm{F} \vdash_{!} v : \{B(r) : T_3 \vee T_5..T_4 \wedge T_6\}$.
- Case (ST$_\#$-Fld): By (VT$_{\#\#}$-Fld).
- Case (ST$_\#$-Met): By (VT$_{\#\#}$-Met).
- Case (ST$_\#$-Eq): By (VT$_{\#\#}$-Eq).
- Case (ST$_\#$-Dist): $T_1 = T_3 \wedge T_4 \vee T_5$. $T_2 = (T_3 \wedge T_4) \vee (T_3 \wedge T_5)$. By 5.63(InvAnd), $\mathrm{F};\rho \vdash_{\#\#} v : T_3$, and $\mathrm{F};\rho \vdash_{\#\#} v : T_4 \vee T_5$. By 5.64(InvOr), $\mathrm{F};\rho \vdash_{\#\#} v : T_4$, or $\mathrm{F};\rho \vdash_{\#\#} v : T_4$. If $\mathrm{F};\rho \vdash_{\#\#} v : T_4$. By (VT$_{\#\#}$-AndI), $\mathrm{F};\rho \vdash_{\#\#} v : T_3 \wedge T_4$. By (VT$_{\#\#}$-Or1), $\mathrm{F};\rho \vdash_{\#\#} v : (T_3 \wedge T_4) \vee (T_3 \wedge T_5)$. Otherwise, $\mathrm{F};\rho \vdash_{\#\#} v : T_5$. By (VT$_{\#\#}$-AndI), $\mathrm{F};\rho \vdash_{\#\#} v : T_3 \wedge T_5$. By (VT$_{\#\#}$-Or2), $\mathrm{F};\rho \vdash_{\#\#} v : (T_3 \wedge T_4) \vee (T_3 \wedge T_5)$.

□

Next, the lemma 5.73(ToInv) shows that tight typing implies invertible typing. The proof is adapted from [4], Theorem 3.6 (page 14).

**Lemma 5.73** (ToInv). *If* $\mathrm{F};\rho \vdash_{\#} v : T$, *where* $\mathrm{F} \sim \rho$, *then* $\mathrm{F};\rho \vdash_{\#\#} v : T$.

*Proof.* Induction on tight variable typing:

- Case (VT$_\#$-Var): $\mathrm{F} = \mathrm{F}_1, v : T, \mathrm{F}_2$. By (VT$_!$-Var), $\mathrm{F} \vdash_{!} v : T$. By (VT$_{\#\#}$-Var), $\mathrm{F};\rho \vdash_{\#\#} v : T$.
- Case (VT$_\#$-RecE): $T = [v/s]T_1$, and $\mathrm{F};\rho \vdash_{\#} v : \mu(s : T_1)$, and $T_1$ **indep** $s$. By induction, $\mathrm{F};\rho \vdash_{\#\#} v : \mu(s : T_1)$. By 5.65(InvRec), $\mathrm{F};\rho \vdash_{\#\#} v : [v/s]T_1$.
- Case (VT$_\#$-RecI): $T = \mu(s : T_1)$, and $\mathrm{F};\rho \vdash_{\#} v : [v/s]T_1$, and $T_1$ **indep** $s$, and $\Gamma;\rho \vdash [v/s]T_1$ **ro** $[v/s]T_1$. By induction, $\mathrm{F};\rho \vdash_{\#\#} v : [v/s]T_1$. By (VT$_{\#\#}$-RecI), $\mathrm{F};\rho \vdash_{\#\#} v : \mu(s : T_1)$.
- Case (VT$_\#$-AndI): $T = T_1 \wedge T_2$, where $\mathrm{F};\rho \vdash_{\#} v : T_1$, and $\mathrm{F};\rho \vdash_{\#} v : T_2$. By induction, $\mathrm{F};\rho \vdash_{\#\#} v : T_1$, and $\mathrm{F};\rho \vdash_{\#\#} v : T_2$. By (VT$_{\#\#}$-AndI), $\mathrm{F};\rho \vdash_{\#} v : T_1 \wedge T_2$.
- Case (VT$_\#$-MutTop): $T = \{\mathsf{M}(r_0) : \bot..\top\}$. By inertness of F, there exist $R$, $s$, $T_1$, such that $\mathrm{F} \vdash_{!} v : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_1\}$. By (VT$_!$-And2), $\mathrm{F} \vdash_{!} v : \{\mathsf{M}(r_0) : \bot..T_1\}$. By (VT$_{\#\#}$-Var), $\mathrm{F};\rho \vdash_{\#\#} v : \{\mathsf{M}(r_0) : \bot..T_1\}$. By (ST$_\#$-Bot) and (ST$_\#$-Top) and (VT$_{\#\#}$-Typ), $\mathrm{F};\rho \vdash_{\#\#} v : \{\mathsf{M}(r_0) : \bot..\top\}$.
- Case (VT$_\#$-Sub): $\mathrm{F};\rho \vdash_{\#} v : T_1$, where $\mathrm{F};\rho \vdash_{\#} T_1 <: T$. By induction, $\mathrm{F};\rho \vdash_{\#\#} v : T_1$. By 5.72(ClInv), $\mathrm{F};\rho \vdash_{\#\#} v : T$.

□

The next lemma shows that a type declaration type given by tight typing implies a type decalaration type given by precise typing, with possibly tighter bounds. The lemma is adapted from [4], page 15.

**Lemma 5.74** (SelP). *If* $\mathrm{F};\rho_1 \vdash_{\#} v : \{B(r) : T_1..T_2\}$, *where* $\mathrm{F} \sim \rho_1$, *then there exist* $T_5$, $T_4$, *such that* $\mathrm{F} \vdash_{!} v : \{B(r) : T_5..T_4\}$, *and* $\mathrm{F};\rho_1 \vdash_{\#} T_1 <: T_5$, *and* $\mathrm{F};\rho_1 \vdash_{\#} T_4 <: T_2$.

*Proof.* By 5.73(ToInv), $\mathrm{F};\rho_1 \vdash_{\#\#} v : \{B(r) : T_1..T_2\}$. By 5.60(InvT). □

The next lemma shows that a type declaration type given by tight typing implies tight subtyping between its bounds and selection of that type member.

This lemma is adapted from [4], Lemma 3.4 (page 12). It is used in 5.76(ToTight).

**Lemma 5.75** (SelR). *If* $\mathrm{F};\rho_1 \vdash_{\#} v : \{B(r) : T_1..T_2\}$, *where* $\mathrm{F} \sim \rho_1$, *then* $\mathrm{F};\rho \vdash_{\#} [x_2/r]T_1 <: v.B(x_2)$, *and* $\mathrm{F};\rho \vdash_{\#} v.B(x_2) <: [x_2/r]T_2$.

*Proof.* By 5.74(SelP), $\mathrm{F} \vdash_{!} v : \{B(r) : T_5..T_4\}$, and $\mathrm{F};\rho \vdash_{\#} T_1 <: T_5$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_2$. By (ST$_\#$-SelL), $\mathrm{F};\rho \vdash_{\#} T_5 <: v.B(x_2)$. By 5.71(SubRTight), $\mathrm{F};\rho \vdash_{\#} [x_2/r]T_1 <: [x_2/r]T_5$. By (ST$_\#$-Trans), $\mathrm{F};\rho \vdash_{\#} [x_2/r]T_1 <: v.B(x_2)$. By (ST$_\#$-SelU), $\mathrm{F};\rho \vdash_{\#} v.B(x_2) <: T_4$. By 5.71(SubRTight), $\mathrm{F};\rho \vdash_{\#} [x_2/r]T_4 <: [x_2/r]T_2$. By (ST$_\#$-Trans), $\mathrm{F};\rho \vdash_{\#} v.B(x_2) <: [x_2/r]T_2$. □

Next, the lemma 5.76(ToTight) shows that variable typing implies tight typing in an inert context. The lemma is adapted from [4], Theorem 3.3 (page 12).

**Lemma 5.76** (ToTight). *If* $\mathrm{F};\rho \vdash v : T$*, where* $\mathrm{F} \sim \rho$*, then* $\mathrm{F};\rho \vdash_{\#} v : T$*. If* $\mathrm{F};\rho \vdash T_1 <: T_2$*, where* $\mathrm{F} \sim \rho$*, then* $\mathrm{F};\rho \vdash_{\#} T_1 <: T_2$*.*

*Proof idea.* Induction on variable typing, term typing and subtyping: For subtyping rules (ST-SelL) and (ST-SelU), use induction on variable typing and 5.75(SelR). For other typing rules, use the same tight typing rule. ▽

*Proof.* Induction on variable typing and subtyping:

- Case (VT-Var): $\mathrm{F} = \mathrm{F}_1, v : T, \mathrm{F}_2$. By (VT$_{\#}$-Var).
- Case (VT-RecE): $\mathrm{F};\rho \vdash v : \mu(s : T_1)$, and $T_1$ **indep** $s$, where $T = [v/s]T_1$. By induction, $\mathrm{F};\rho \vdash_{\#} v : \mu(s : T_1)$. By (VT$_{\#}$-RecE).
- Case (VT-RecI): $\mathrm{F};\rho \vdash v : [s/v]T_1$, and $T_1$ **indep** $s$, and $\mathrm{F};\rho \vdash [s/v]T_1$ **ro** $[s/v]T_1$, where $T = \mu(s : T_1)$. By induction, $\mathrm{F};\rho \vdash_{\#} v : [s/v]T_1$. By (VT$_{\#}$-RecI).
- Case (VT-AndI): $\mathrm{F};\rho \vdash v : T_1$, and $\mathrm{F};\rho \vdash v : T_2$, where $T = T_1 \wedge T_2$. By induction, $\mathrm{F};\rho \vdash_{\#} v : T_1$, and $\mathrm{F};\rho \vdash_{\#} v : T_2$. By (VT$_{\#}$-AndI).
- Case (VT-MutTop): $T = \{\mathsf{M}(r_0) : \bot..\top\}$. By (VT$_{\#}$-MutTop).
- Case (VT-Sub): $\mathrm{F};\rho \vdash v : T_1$, where $\mathrm{F};\rho \vdash T_1 <: T$. By induction, $\mathrm{F};\rho \vdash_{\#} v : T_1$, and $\mathrm{F};\rho \vdash_{\#} T_1 <: T$. By (VT$_{\#}$-Sub).
- Case (ST-Top): $T_2 = \top$. By (ST$_{\#}$-Top).
- Case (ST-Bot): $T_1 = \bot$. By (ST$_{\#}$-Bot).
- Case (ST-Refl): $T_1 = T_2$. By (ST$_{\#}$-Refl).
- Case (ST-N-Rec): $T_1 = \mathsf{N}$, and $T_2 = \mu(s : T_3)$. By (ST$_{\#}$-N-Rec).
- Case (ST-N-M): $T_1 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_2 = \bot$. By (ST$_{\#}$-N-M).
- Case (ST-And1): $T_1 = T_2 \wedge T_3$. By (ST$_{\#}$-And1).
- Case (ST-And2): $T_1 = T_3 \wedge T_2$. By (ST$_{\#}$-And2).
- Case (ST-And): $\mathrm{F};\rho \vdash T_1 <: T_3$, and $\mathrm{F};\rho \vdash T_1 <: T_4$, where $T_2 = T_3 \wedge T_4$. By induction, $\mathrm{F};\rho \vdash_{\#} T_1 <: T_3$, and $\mathrm{F};\rho \vdash_{\#} T_1 <: T_4$. By (ST$_{\#}$-And).
- Case (ST-Or1): $T_2 = T_1 \vee T_3$. By (ST$_{\#}$-Or1).
- Case (ST-Or2): $T_2 = T_3 \vee T_1$. By (ST$_{\#}$-Or2).
- Case (ST-Or): $\mathrm{F};\rho \vdash T_3 <: T_2$, and $\mathrm{F};\rho \vdash T_4 <: T_2$, where $T_1 = T_3 \vee T_4$. By induction, $\mathrm{F};\rho \vdash_{\#} T_3 <: T_2$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_2$. By (ST$_{\#}$-Or).
- Case (ST-Trans): $\mathrm{F};\rho \vdash T_1 <: T_3$, and $\mathrm{F};\rho \vdash T_2 <: T_3$. By induction, $\mathrm{F};\rho \vdash_{\#} T_1 <: T_3$, and $\mathrm{F};\rho \vdash_{\#} T_2 <: T_3$. By (ST$_{\#}$-Trans).
- Case (ST-SelL): $T_2 = x_1.B(x_2)$, and $T_1 = [x_2/r]T_3$, where $\mathrm{F};\rho \vdash x_1 : \{B(r) : T_3..T_4\}$. By 5.75(SelR).
- Case (ST-SelU): $T_1 = x_1.B(x_2)$, and $T_2 = [x_2/r]T_4$, where $\mathrm{F};\rho \vdash x_1 : \{B(r) : T_3..T_4\}$. By 5.75(SelR).
- Case (ST-Typ): $T_1 = \{B(r) : T_3..T_4\}$, and $T_2 = \{B(r) : T_5..T_6\}$, where $\mathrm{F};\rho \vdash T_5 <: T_3$, and $\mathrm{F};\rho \vdash T_4 <: T_6$. By induction, $\mathrm{F};\rho \vdash_{\#} T_5 <: T_3$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_6$. By (ST$_{\#}$-Typ).
- Case (ST-Fld): $T_1 = \{a : T_3..T_4\}$, and $T_2 = \{a : T_5..T_6\}$, where $\mathrm{F};\rho \vdash T_5 <: T_3$, and $\mathrm{F};\rho \vdash T_4 <: T_6$. By induction, $\mathrm{F};\rho \vdash_{\#} T_5 <: T_3$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_6$. By (ST$_{\#}$-Fld).
- Case (ST-Met): $T_1 = \{m(z : T_3, r : T_5) : T_4\}$, and $T_2 = \{m(z : T_6, r : T_8) : T_7\}$, where $\mathrm{F};\rho \vdash T_6 <: T_3$, and $\mathrm{F}, z : T_6;\rho \vdash T_8 <: T_5$, and $\mathrm{F}, z : T_6, r : T_8;\rho \vdash T_4 <: T_7$. By induction, $\mathrm{F};\rho \vdash_{\#} T_6 <: T_3$. By (ST$_{\#}$-Met).
- Case (ST-TypAnd): $T_1 = \{B(r) : T_3..T_4\} \wedge \{B(r) : T_5..T_6\}$, and $T_2 = \{B(r) : T_3 \vee T_5..T_4 \wedge T_6\}$. By (ST$_{\#}$-TypAnd).
- Case (ST-Eq): $\rho \vdash T_1 \approx T_2$. By (ST$_{\#}$-Eq).
- Case (ST-N-Fld): $T_1 = \mathsf{N}$, and $T_2 = \{a : T_3..T_4\}$. By (ST$_{\#}$-N-Fld).
- Case (ST-N-Met): $T_1 = \mathsf{N}$, and $T_2 = \{m(z : T_3, r : T_5) : T_4\}$. By (ST$_{\#}$-N-Met).

- Case (ST-N-Typ): $T_1 = \mathsf{N}$, and $T_2 = \{B(r) : T_3..T_4\}$. By (ST$_\#$-N-Typ).
- Case (ST-Dist): $T_1 = T_3 \wedge T_4 \vee T_5$, and $T_2 = T_3 \wedge T_4 \vee T_3 \wedge T_5$. By (ST$_\#$-Dist).

□

**Lemma 5.77** (VTEq)**.** *If* $\mathrm{F};\rho \vdash v : T$*, where* $\mathrm{F} \sim \rho$*, then* $\mathrm{F};\rho \vdash_{\#\#} v : T$*.*

*Idea.* In an inert context, normal typing implies invertible typing. ▽

*Proof.* By 5.76(ToTight), $\mathrm{F};\rho \vdash_{\#} v : T$. By 5.73(ToInv), $\mathrm{F};\rho \vdash_{\#\#} v : T$. □

The following lemmata show the opposite direction of the equivalence, going from precise and invertible typing to normal typing.

**Lemma 5.78** (VTEqB)**.** *If* $\mathrm{F} \vdash_{!} v : T$*, then* $\mathrm{F};\rho \vdash v : T$*.*

*Idea.* In an inert context, precise typing implies normal typing. ▽

*Proof.* Induction on precise typing:

- Case (VT$_!$-Var): $\mathrm{F} = \mathrm{F}_1, v : T, \mathrm{F}_2$. By (VT-Var).
- Case (VT$_!$-Rec): $T = [v/s]T_1$, and $\mathrm{F} \vdash_{!} v : \mu(s : T_1)$. By 5.48(PrecForms) and by inertness of F, $T_1$ **indep** $s$. By (VT-RecE).
- Case (VT$_!$-And1): $\mathrm{F} \vdash_{!} v : T \wedge T_1$. By induction, $\mathrm{F};\rho \vdash v : T \wedge T_1$. By (ST-And1), $\mathrm{F};\rho \vdash T \wedge T_1 <: T$. By (VT-Sub), $\mathrm{F};\rho \vdash v : T$.
- Case (VT$_!$-And2): $\mathrm{F} \vdash_{!} v : T_1 \wedge T$. By induction, $\mathrm{F};\rho \vdash v : T_1 \wedge T$. By (ST-And2), $\mathrm{F};\rho \vdash T_1 \wedge T <: T$. By (VT-Sub), $\mathrm{F};\rho \vdash v : T$.

□

**Lemma 5.79** (STEqB)**.** *If* $\mathrm{F};\rho \vdash_{\#} T_1 <: T_2$*, then* $\mathrm{F};\rho \vdash T_1 <: T_2$*.*

*Proof.* Induction on tight subtyping:

- Cases (ST$_\#$-SelU), (ST$_\#$-SelL): By 5.78(VTEqB) and (ST-SelU) or by (ST-SelL).
- Other cases straightforward by induction and the corresponding subtyping rule.

□

**Lemma 5.80** (FromInv)**.** *If* $\mathrm{F};\rho \vdash_{\#\#} v : T$*, then* $\mathrm{F};\rho \vdash v : T$*.*

*Proof.* Induction on $\mathrm{F};\rho \vdash_{\#\#} v : T$:

- Case (VT$_{\#\#}$-Var): $\mathrm{F} \vdash_{!} v : T$. By 5.78(VTEqB).
- Case (VT$_{\#\#}$-Top): $\mathrm{F} \vdash_{!} v : T_1$, and $T = \top$. By (ST-Top). $\mathrm{F};\rho \vdash T_1 <: T$. By (VT-Sub).
- Case (VT$_{\#\#}$-AndI): $T = T_1 \wedge T_2$, and $\mathrm{F};\rho \vdash_{\#\#} v : T_1$, and $\mathrm{F};\rho \vdash_{\#\#} v : T_2$. By induction, $\mathrm{F};\rho \vdash v : T_1$, and $\mathrm{F};\rho \vdash v : T_2$. By (VT-AndI).
- Case (VT$_{\#\#}$-Or1): $T = T_1 \vee T_2$, and $\mathrm{F};\rho \vdash_{\#\#} v : T_1$. By induction, $\mathrm{F};\rho \vdash v : T_1$. By (ST-Or1), $\mathrm{F};\rho \vdash T_1 <: T$. By (VT-Sub).
- Case (VT$_{\#\#}$-Or2): $T = T_1 \vee T_2$, and $\mathrm{F};\rho \vdash_{\#\#} v : T_2$. By induction, $\mathrm{F};\rho \vdash v : T_2$. By (ST-Or2), $\mathrm{F};\rho \vdash T_2 <: T$. By (VT-Sub).
- Case (VT$_{\#\#}$-RecI): $T = \mu(s : T_1)$, and $\mathrm{F};\rho \vdash_{\#\#} v : [v/s]T_1$, and $T_1$ **indep** $s$, and $\mathrm{F};\rho \vdash [v/s]T_1$ **ro** $[v/s]T_1$. By induction, $\mathrm{F};\rho \vdash v : [v/s]T_1$. By (VT-RecI).
- Case (VT$_{\#\#}$-Sel): $T = v_2.B(x)$, and $\mathrm{F};\rho \vdash_{\#\#} v : [x/r]T_1$, and $\mathrm{F} \vdash_{!} v_2 : \{B(r) : T_1..T_2\}$. By induction, $\mathrm{F};\rho \vdash v : [x/r]T_1$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash v_2 : \{B(r) : T_1..T_2\}$. By (ST-SelL), $\mathrm{F};\rho \vdash [x/r]T_1 <: T$. By (VT-Sub).
- Case (VT$_{\#\#}$-Typ): $T = \{B(r) : T_1..T_2\}$, and $\mathrm{F};\rho \vdash_{\#\#} v : \{B(r) : T_3..T_4\}$, and $\mathrm{F};\rho \vdash_{\#} T_1 <: T_3$, and $\mathrm{F};\rho \vdash_{\#} T_4 <: T_2$. By induction, $\mathrm{F};\rho \vdash v : \{B(r) : T_3..T_4\}$. By 5.79(STEqB), $\mathrm{F};\rho \vdash T_1 <: T_3$, and $\mathrm{F};\rho \vdash T_4 <: T_2$. By (ST-Typ), $\mathrm{F};\rho \vdash \{B(r) : T_3..T_4\} <: T$. By (VT-Sub).

- Case (VT$_{\#\#}$-Met): $T = \{m(z : T_1, r : T_3) : T_2\}$, and F;$\rho \vdash_{\#\#} v : \{m(z : T_5, r : T_6) : T_4\}$, and F;$\rho \vdash_{\#} T_1 <: T_3$, and $\mathrm{F}, z : T_1$;$\rho \vdash T_3 <: T_6$, and $\mathrm{F}, z : T_1, r : T_3$;$\rho \vdash T_4 <: T_2$. By induction, F;$\rho \vdash v : \{m(z : T_5, r : T_6) : T_4\}$. By 5.79(STEqB), F;$\rho \vdash T_1 <: T_3$. By (ST-Met), F;$\rho \vdash \{m(z : T_5, r : T_6) : T_4\} <: T$. By (VT-Sub).
- Case (VT$_{\#\#}$-Fld): $T = \{a : T_1..T_2\}$, and F;$\rho \vdash_{\#\#} v : \{a : T_3..T_4\}$, and F;$\rho \vdash_{\#} T_1 <: T_3$, and F;$\rho \vdash_{\#} T_4 <: T_2$. By induction, F;$\rho \vdash v : \{a : T_3..T_4\}$. By 5.79(STEqB), F;$\rho \vdash T_1 <: T_3$, and F;$\rho \vdash T_4 <: T_2$. By (ST-Fld), F;$\rho \vdash \{a : T_3..T_4\} <: T$. By (VT-Sub).
- Case (VT$_{\#\#}$-Eq): $\rho \vdash T \approx T_1$, and F;$\rho \vdash_{\#\#} v : T_1$. By induction, F;$\rho \vdash v : T_1$. By (ST-Eq) and (VT-Sub).

□

### 5.2.6 Reference lemmata

This section contains lemmata about deriving typing relations involving references ($w$) from typing relations involving the corresponding location ($y$, when $w \rightarrow y \in \rho$).

**Lemma 5.81** (EqRO)**.** *If* $\mathrm{F};\rho \vdash T_1$ **ro** $T_2$*, and* $\rho \vdash T_1 \approx T_3$*, and* $\mathrm{F} \sim \rho$*, then there exists* $T_4$*, such that* $\mathrm{F};\rho \vdash T_3$ **ro** $T_4$*, and* $\rho \vdash T_2 \approx T_4$*.*

*Proof.* Induction on $\mathrm{F} \vdash T_1 \approx T_3$:

- Case (TE-Refl): $T_1 = T_3$. Choose $T_4 = T_2$. By (TE-Refl).
- Case (TE-Sel): $T_1 = v_1.A(x_2)$, and $T_3 = v_2.A(x_2)$, where $\rho \vdash v_1 \approx v_2$. By inversion of (TS-Sel), $\mathrm{F} \vdash_! v_1 : \{A(r) : T_5..T_6\}$, where $\mathrm{F};\rho \vdash T_6$ **ro** $T_2$. By 5.55(EqPrecTyp), $\mathrm{F} \vdash_! v_2 : \{A(r) : T_7..T_8\}$, where $\rho \vdash T_6 \approx T_8$. By induction, exists $T_4$, such that $\mathrm{F};\rho \vdash T_8$ **ro** $T_4$, and $\rho \vdash T_2 \approx T_4$. By (TS-Sel), $\mathrm{F};\rho \vdash T_3$ **ro** $T_4$.
- Case (TE-And): $T_1 = T_5 \wedge T_6$, and $T_2 = T_7 \wedge T_8$, and $\rho \vdash T_3 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of (TS-AndR), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \wedge T_{10}$, and $\mathrm{F};\rho \vdash T_5$ **ro** $T_9$, and $\mathrm{F};\rho \vdash T_6$ **ro** $T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F};\rho \vdash T_9$ **ro** $T_{11}$, and $\mathrm{F};\rho \vdash T_{10}$ **ro** $T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \wedge T_{12}$. By (TE-And) and (TS-AndR).
- Case (TE-Or): $T_1 = T_5 \vee T_6$, and $T_2 = T_7 \vee T_8$, and $\rho \vdash T_3 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of (TS-OrR), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \vee T_{10}$, and $\mathrm{F};\rho \vdash T_5$ **ro** $T_9$, and $\mathrm{F};\rho \vdash T_6$ **ro** $T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F};\rho \vdash T_9$ **ro** $T_{11}$, and $\mathrm{F};\rho \vdash T_{10}$ **ro** $T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \vee T_{12}$. By (TE-Or) and (TS-OrR).
- Case (TE-Rec): $T_1 = \mu(s : T_5)$, and $T_3 = \mu(s : T_7)$, and $\rho \vdash T_5 \approx T_7$. By inversion of (TS-Rec), $T_2 = T_1$. Choose $T_4 = T_3$. By (TS-Rec).
- Case (TE-Typ): $T_1 = \{A(r) : T_5..T_6\}$, and $T_3 = \{A(r) : T_7..T_8\}$. By inversion of (TS-Typ), $T_2 = T_1$. Choose $T_4 = T_3$. By (TS-Typ).
- Case (TE-Fld): $T_1 = \{a : T_5..T_6\}$, and $T_3 = \{a : T_7..T_8\}$. By inversion of (TS-Fld), $T_2 = T_1$. Choose $T_4 = T_3$. By (TS-Fld).
- Case (TE-Met): $T_1 = \{m(z : T_5, r : T_7) : T_6\}$, and $T_3 = \{m(z : T_8, r : T_{10}) : T_9\}$. By inversion of (TS-Met), $T_2 = T_1$. Choose $T_4 = T_3$. By (TS-Met).

□

**Lemma 5.82** (RefPrecRec)**.** *If* $\mathrm{F} \vdash_! y : \mu(s : T_1)$*, and* $w \rightarrow y \in \rho$*, and* $\mathrm{F} \sim \rho$*, then* $\mathrm{F} \vdash_! w : \mu(s : T_1)$*.*

*Idea.* Precise recusive type of a reference is the same as the precise types of the corresponding location. ▽

*Proof.* By 5.48(PrecForms), $\mathrm{F} = \mathrm{F}_1, y : \mu(s : T_1) \wedge \{\mathsf{M}(r_0) : \bot..T_2\}, \mathrm{F}_2$. By 5.17(ECorrInvW), $\mathrm{F}_2 = \mathrm{F}_3, w : \mu(s : T_1) \wedge \{\mathsf{M}(r_0) : \bot..T_3\}, \mathrm{F}_4$. By (VT$_!$-Var) and (VT$_!$-And1), $\mathrm{F} \vdash_! w : \mu(s : T_1)$. □

**Lemma 5.83** (RefPrecFld)**.** *If* $\mathrm{F} \vdash_! y : \{a : T_1..T_2\}$*, and* $w \rightarrow y \in \rho$*, and* $\mathrm{F} \sim \rho$*, then* $\mathrm{F} \vdash_! w : \{a : T_3..T_4\}$*, where* $\rho \vdash T_1 \approx T_3$*, and* $\rho \vdash T_4 \approx T_2$*.*

*Idea.* Precise types of fields of a reference are equivalent to the precise types of the corresponding location. ▽

*Proof.* By 5.50(PrecSim), $\mathrm{F} \vdash_{!1} y : \{a : T_1..T_2\}$. By inversion of (VT$_{!1}$-Var), $\mathrm{F} = \mathrm{F}_1, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$, where $[y/s]R = \ldots_1 \{a : T_1..T_2\} \ldots_2$. By 5.17(ECorrInvW), $\mathrm{F}_2 = \mathrm{F}_3, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_7\}, \mathrm{F}_4$. Choose $T_3$, and $T_4$, such that $R = \ldots_5 \{a : T_5..T_6\} \ldots_6$, and $T_3 = [w/s]T_5$, and $T_4 = [w/s]T_6$, therefore $[w/s]R = \ldots_3 \{a : T_3..T_4\} \ldots_4$. By inertness of F, $R$ **indep** $s$, therefore $T_5$ **indep** $s$, and $T_6$ **indep** $s$. By 5.67(IndepEq), $\rho \vdash T_1 \approx T_3$, and $\rho \vdash T_2 \approx T_4$. By (VT$_{!1}$-Var), $\mathrm{F} \vdash_{!1} w : \{a : T_3..T_4\}$. By 5.51(PrecSimInv), $\mathrm{F} \vdash_! w : \{a : T_3..T_4\}$. □

**Lemma 5.84** (RefPrecMet)**.** *If* $\mathrm{F} \vdash_! y : \{m(z : T_1, r : T_3) : T_2\}$*, and* $w \rightarrow y \in \rho$*, and* $\mathrm{F} \sim \rho$*, then* $\mathrm{F} \vdash_! w : \{m(z : T_4, r : T_6) : T_5\}$*, where* $\rho \vdash T_4 \approx T_1$*, and* $\rho \vdash T_5 \approx T_2$*, and* $\rho \vdash T_6 \approx T_3$*.*

*Idea.* Precise types of methods of a reference are equivalent to the precise types of the corresponding location. ▽

*Proof.* By 5.50(PrecSim), $\mathrm{F} \vdash_{!1} y : \{m(z : T_1, r : T_3) : T_2\}$. By inversion of (VT$_{!1}$-Var), $\mathrm{F} = \mathrm{F}_1, y : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$, where $[y/s]R = \ldots_1 \{m(z : T_1, r : T_3) : T_2\} \ldots_2$, and $y \notin \mathrm{dom}\ \mathrm{F}_2$. By 5.17(ECorrInvW), $\mathrm{F}_2 = \mathrm{F}_3, w : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..T_{10}\}, \mathrm{F}_4$. Choose $T_4$, and $T_5$, and $T_6$, such that $R = \ldots_5 \{m(z : T_7, r : T_9) : T_8\} \ldots_6$, and $T_4 = [w/s]T_7$, and $T_5 = [w/s]T_8$, and $T_6 = [w/s]T_9$, therefore $[w/s]R = \ldots_3 \{m(z : T_4, r : T_6) : T_5\} \ldots_4$. By inertness of F, $R$ **indep** $s$, therefore $T_7$ **indep** $s$, and $T_8$ **indep** $s$, and $T_9$ **indep** $s$. By 5.67(IndepEq), $\rho \vdash T_1 \approx T_4$, and $\rho \vdash T_2 \approx T_5$, and $\rho \vdash T_3 \approx T_6$. By (VT$_{!1}$-Var), $\mathrm{F} \vdash_{!1} w : \{m(z : T_4, r : T_6) : T_5\}$. By 5.51(PrecSimInv), $\mathrm{F} \vdash_{!} w : \{m(z : T_4, r : T_6) : T_5\}$. □

**Lemma 5.85** (RefPrecTyp). *If* $\mathrm{F} \vdash_{!} y : \{A(r) : T_1..T_2\}$, *and* $w \to y \in \rho$, *and* $\mathrm{F} \sim \rho$, *then* $\mathrm{F} \vdash_{!} w : \{A(r) : T_3..T_4\}$, *where* $\rho \vdash T_3 \approx T_1$, *and* $\rho \vdash T_4 \approx T_2$.

*Idea.* Precise types of normal type members of a reference are equivalent to the precise types of the corresponding location. ▽

*Proof.* By 5.54(EqPrecTypL). □

**Lemma 5.86** (RefPrecRecord). *If* $\mathrm{F} \vdash_{!} y : R_1$, *and* $w \to y \in \rho$, *and* $\mathrm{F} \sim \rho$, *then* $\mathrm{F};\rho \vdash w : R_1$.

*Proof.* Induction on $R_1$:

- If $R_1 = R_2 \wedge R_3$. By (VT$_!$-And1), $\mathrm{F} \vdash_{!} y : R_2$, and $\mathrm{F} \vdash_{!} y : R_3$. By induction, $\mathrm{F};\rho \vdash w : R_2$, and $\mathrm{F};\rho \vdash w : R_3$. By (VT-AndI), $\mathrm{F};\rho \vdash w : R_1$.
- If $R_1 = \{a : T_1..T_1\}$. By 5.83(RefPrecFld) and (TE-Fld), $\mathrm{F} \vdash_{!} w : R_2$, where $\rho \vdash R_1 \approx R_2$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash w : R_2$. By (ST-Eq) and (VT-Sub), $\mathrm{F};\rho \vdash w : R_1$.
- If $R_1 = \{A(r) : T_1..T_2\}$. By 5.85(RefPrecTyp) and (TE-Typ), $\mathrm{F} \vdash_{!} w : R_2$, where $\rho \vdash R_1 \approx R_2$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash w : R_2$. By (ST-Eq) and (VT-Sub), $\mathrm{F};\rho \vdash w : R_1$.
- If $R_1 = \{m(z : T_1, r : T_3) : T_2\}$. By 5.84(RefPrecMet) and (TE-Met), $\mathrm{F} \vdash_{!} w : R_2$, where $\rho \vdash R_1 \approx R_2$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash w : R_2$. By (ST-Eq) and (VT-Sub), $\mathrm{F};\rho \vdash w : R_1$.

□

**Lemma 5.87** (RefT). *If* $\mathrm{F};\rho \vdash y : T_1$, *and* $\mathrm{F};\rho \vdash T_1$ **ro** $T_2$, *and* $\mathrm{F} \sim \rho$, *and* $w \to y \in \rho$, *then* $\mathrm{F};\rho \vdash w : T_2$.

*Idea.* $w$ has the read-only part of the type $y$ has. ▽

*Proof.* Induction on splitting and invertible typing. By 5.77(VTEq), $\mathrm{F};\rho \vdash_{\#\#} y : T_1$. If that is by (VT$_{\#\#}$-Eq), then $\mathrm{F};\rho \vdash_{\#\#} y : T_3$, where $\rho \vdash T_3 \approx T_1$. By 5.2(EqSymm), $\rho \vdash T_1 \approx T_3$. By 5.81(EqRO), exists $T_4$, such that $\mathrm{F};\rho \vdash T_3$ **ro** $T_4$, and $\rho \vdash T_2 \approx T_4$. By induction, $\mathrm{F};\rho \vdash w : T_4$. By 5.2(EqSymm), $\rho \vdash T_4 \approx T_2$. By (VT$_{\#\#}$-Eq), $\mathrm{F};\rho \vdash w : T_2$. Otherwise induction on $\mathrm{F};\rho \vdash T_1$ **ro** $T_2$:

- Case (TS-Top): $T_2 = \top$. By (ST-Top) and (VT-Sub).
- Case (TS-Bot): $T_1 = \bot$. Not possible by 5.59(NoInvTyp).
- Case (TS-M): $T_2 = \top$. By (ST-Top) and (VT-Sub).
- Case (TS-Typ): $T_1 = T_2 = \{A(r) : T_3..T_4\}$. By 5.60(InvT), $\mathrm{F} \vdash_{!} y : \{A(r) : T_5..T_6\}$, and $\mathrm{F};\rho \vdash T_3 <: T_5$, and $\mathrm{F};\rho \vdash T_6 <: T_4$. By 5.85(RefPrecTyp), $\mathrm{F} \vdash_{!} w : \{A(r) : T_7..T_8\}$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_8 \approx T_6$. By (ST-Eq), $\mathrm{F};\rho \vdash T_5 <: T_7$, and $\mathrm{F};\rho \vdash T_8 <: T_6$. By (ST-Trans), $\mathrm{F};\rho \vdash T_3 <: T_7$, and $\mathrm{F};\rho \vdash T_8 <: T_4$. By (ST-Typ), $\mathrm{F};\rho \vdash \{A(r) : T_7..T_8\} <: T_2$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash w : \{A(r) : T_7..T_8\}$. By (VT-Sub), $\mathrm{F};\rho \vdash w : T_2$.
- Case (TS-Fld): $T_1 = T_2 = \{a : T_3..T_4\}$. By 5.61(InvF), $\mathrm{F} \vdash_{!} y : \{a : T_5..T_6\}$, and $\mathrm{F};\rho \vdash T_3 <: T_5$, and $\Gamma;\rho \vdash T_6 <: T_4$. By 5.83(RefPrecFld), $\mathrm{F} \vdash_{!} w : \{a : T_7..T_8\}$, and $\mathrm{F} \vdash T_5 \approx T_7$, and $\mathrm{F} \vdash T_8 \approx T_6$. By (ST-Eq), $\mathrm{F};\rho \vdash T_5 <: T_7$, and $\mathrm{F};\rho \vdash T_8 <: T_6$. By (ST-Trans), $\mathrm{F};\rho \vdash T_3 <: T_7$, and $\mathrm{F};\rho \vdash T_8 <: T_4$. By (ST-Fld), $\mathrm{F};\rho \vdash \{a : T_7..T_8\} <: T_2$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash w : \{a : T_7..T_8\}$. By (VT-Sub), $\mathrm{F};\rho \vdash w : T_2$.
- Case (TS-Met): $T_1 = T_2 = \{m(z : T_3, r : T_5) : T_4\}$. By 5.62(InvM), $\mathrm{F} \vdash_{!} y : \{m(z : T_6, r : T_8) : T_7\}$, and $\mathrm{F};\rho \vdash T_3 <: T_6$, and $\mathrm{F}, z : T_3;\rho \vdash T_7 <: T_4$, and $\mathrm{F}, z : T_3;\rho \vdash T_8 <: T_5$. By 5.84(RefPrecMet), $\mathrm{F} \vdash_{!} w : \{m(z : T_9, r : T_{11}) : T_{10}\}$, and $\rho \vdash T_6 \approx T_9$, and $\rho \vdash T_{10} \approx T_7$, and $\rho \vdash T_{11} \approx T_8$. By (ST-Eq), $\mathrm{F};\rho \vdash T_6 <: T_9$, and $\mathrm{F}, z : T_3;\rho \vdash T_{10} <: T_7$, and $\mathrm{F}, z : T_3;\rho \vdash T_{11} <: T_8$. By (ST-Trans), $\mathrm{F};\rho \vdash T_3 <: T_9$, and $\mathrm{F}, z : T_3;\rho \vdash T_{10} <: T_4$, and $\mathrm{F}, z : T_3;\rho \vdash T_{11} <: T_5$. By (ST-Met), $\mathrm{F};\rho \vdash \{m(z : T_9, r : T_{11}) : T_{10}\} <: T_2$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash w : \{m(z : T_9, r : T_{11}) : T_{10}\}$. By (VT-Sub), $\mathrm{F};\rho \vdash w : T_2$.

- Case (TS-Rec): $T_1 = T_2 = \mu(s : T_3)$. By inversion: Subcase (VT$_{\#\#}$-Var): $\mathrm{F} \vdash_! y : T_1$. By 5.82(RefPrecRec), $\mathrm{F} \vdash_! w : T_1$. Subcase (VT$_{\#\#}$-RecI): $\mathrm{F};\rho \vdash_{\#\#} y : [y/s]T_3$, and $T_3$ **indep** $s$, and $\mathrm{F};\rho \vdash [y/s]T_3$ **ro** $[y/s]T_3$. By induction, $\mathrm{F};\rho \vdash_{\#\#} w : [y/s]T_3$. By 5.67(IndepEq), $\mathrm{F} \vdash [y/s]T_3 \approx [w/s]T_3$ and (ST-Eq) and (VT-Sub), $\mathrm{F};\rho \vdash_{\#\#} y : [y/s]T_3$. By (VT-RecI), $\mathrm{F};\rho \vdash y : \mu(s : T_3)$.
- Case (TS-Sel): $T_1 = x.B(x_2)$, and $\mathrm{F};\rho \vdash x : \{B(r) : T_3..T_4\}$, and $\mathrm{F};\rho \vdash [x_2/r]T_4$ **ro** $T_2$. By inversion: Subcase (VT$_{\#\#}$-Var): $\mathrm{F} \vdash_! y : T_1$. Not possible by 5.49(NoPrecTyp). Subcase (VT$_{\#\#}$-Sel): $\mathrm{F} \vdash_! x : \{B(r) : T_5..T_6\}$. $\mathrm{F};\rho \vdash_{\#\#} y : [x_2/r]T_5$. By 5.77(VTEq), $\mathrm{F};\rho \vdash_{\#\#} x : \{B(r) : T_3..T_4\}$. By 5.60(InvT), exist $T_7$, $T_8$, such that $\mathrm{F} \vdash_! x : \{B(r) : T_7..T_8\}$, and $\mathrm{F};\rho \vdash_{\#} T_3 <: T_7$, and $\mathrm{F};\rho \vdash_{\#} T_8 <: T_4$. By 5.52(UPrecTyp), $T_7 = T_5$, and $T_8 = T_6$. By 5.53(SubPrecTyp), either $T_5 = \bot$, or $T_5 = T_6$. By 5.59(NoInvTyp), $T_5 \neq \bot$, so $T_5 = T_6$, therefore $\mathrm{F};\rho \vdash_{\#\#} y : [x_2/r]T_6$. By 5.71(SubRTight), $\mathrm{F};\rho \vdash_{\#} [x_2/r]T_6 <: [x_2/r]T_4$. By 5.72(ClInv), $\mathrm{F};\rho \vdash_{\#\#} y : [x_2/r]T_4$. By 5.80(FromInv), $\mathrm{F};\rho \vdash y : [x_2/r]T_4$. By induction, $\mathrm{F};\rho \vdash w : T_2$.
- Case (TS-AndR): $T_1 = T_3 \wedge T_4$, and $T_2 = T_5 \wedge T_6$, where $\mathrm{F};\rho \vdash T_3$ **ro** $T_5$, and $\mathrm{F};\rho \vdash T_4$ **ro** $T_6$. By inversion: Subcase (VT$_{\#\#}$-Var): $\mathrm{F} \vdash_! y : T_1$. By 5.48(PrecForms), either exist $s$, $R$, $T_7$, such that $T_3 = \mu(s : R)$, and $T_4 = \{\mathsf{M}(r_0) : \bot..T_7\}$, or exists $R$, such that $T_1 = R$. If $T_1 = R$, then by 5.86(RefPrecRecord), $\mathrm{F};\rho \vdash w : R$. By 5.37(RecordRO), $T_2 = T_1$. Otherwise. By inversion of (TS-M), $T_6 = \top$. By inversion of (TS-Rec), $T_5 = T_3$. By (VT$_!$-And1), $\mathrm{F} \vdash_! y : T_3$. By 5.82(RefPrecRec), $\mathrm{F} \vdash_! w : T_5$. By 5.78(VTEqB), $\mathrm{F};\rho \vdash w : T_5$. By (ST-Top) and (VT-Sub) and (VT-AndI), $\mathrm{F};\rho \vdash w : T_5 \wedge T_6$. Subcase (VT$_{\#\#}$-AndI), $\mathrm{F};\rho \vdash_{\#\#} y : T_3$, and $\mathrm{F};\rho \vdash_{\#\#} y : T_4$: By induction, $\mathrm{F};\rho \vdash w : T_5$, and $\mathrm{F};\rho \vdash w : T_6$. By (VT-AndI), $\mathrm{F};\rho \vdash w : T_2$.
- Case (TS-OrR): $T_1 = T_3 \vee T_4$. $T_2 = T_5 \vee T_6$, where $\mathrm{F};\rho \vdash T_3$ **ro** $T_5$, and $\mathrm{F};\rho \vdash T_4$ **ro** $T_6$. By inversion: Subcase (VT$_{\#\#}$-Var): Not possible by 5.49(NoPrecTyp). Subcase (VT$_{\#\#}$-Or1): $\mathrm{F};\rho \vdash_{\#\#} y : T_3$. By induction, $\mathrm{F};\rho \vdash w : T_5$. By (ST-Or1), $\mathrm{F};\rho \vdash T_5 <: T_2$. By (VT-Sub), $\mathrm{F};\rho \vdash w : T_2$. Subcase (VT$_{\#\#}$-Or2): $\mathrm{F};\rho \vdash_{\#\#} y : T_4$. By induction, $\mathrm{F};\rho \vdash y : T_6$. By (ST-Or2), $\mathrm{F};\rho \vdash T_6 <: T_2$. By (VT-Sub), $\mathrm{F};\rho \vdash w : T_2$.

□

### 5.2.7 Restricted Subtyping Lemmata

This section contains lemmata about restricted versions of tight subtyping, defined in sections 4.11 and 4.12, and how they commute with relations $\vdash\!\longmapsto^{\mathrm{s}}$, $\longmapsto^{\mathrm{m}}$ and $\longmapsto^{\mathrm{e}}$ defined in sections 4.8, 4.9 and 4.10.

**Lemma 5.88** (AndSubS). *If* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_3$*, and* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_2 <: T_4$*, then* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \wedge T_2 <: T_3 \wedge T_4$*.*

*Proof.* By (ST$^{\mathrm{s}}_{\#}$-And1), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \wedge T_2 <: T_1$, by (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \wedge T_2 <: T_3$. By (ST$^{\mathrm{s}}_{\#}$-And2), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \wedge T_2 <: T_2$, by (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \wedge T_2 <: T_4$. By (ST$^{\mathrm{s}}_{\#}$-And), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \wedge T_2 <: T_3 \wedge T_4$. □

**Lemma 5.89** (OrSubS). *If* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_3$*, and* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_2 <: T_4$*, then* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \vee T_2 <: T_3 \vee T_4$*.*

*Proof.* By (ST$^{\mathrm{s}}_{\#}$-Or1), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_3 <: T_3 \vee T_4$, by (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_3 \vee T_4$. By (ST$^{\mathrm{s}}_{\#}$-Or2), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_4 <: T_3 \vee T_4$, by (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_2 <: T_3 \vee T_4$. By (ST$^{\mathrm{s}}_{\#}$-Or), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 \vee T_2 <: T_3 \vee T_4$. □

**Lemma 5.90** (AndSubM). *If* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_3$*, and* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_4$*, then* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_3 \wedge T_4$*.*

*Proof.* By (ST$^{\mathrm{m}}_{\#}$-And1), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_1$, by (ST$^{\mathrm{m}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_3$. By (ST$^{\mathrm{m}}_{\#}$-And2), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_2$, by (ST$^{\mathrm{m}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_4$. By (ST$^{\mathrm{m}}_{\#}$-And), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \wedge T_2 <: T_3 \wedge T_4$. □

**Lemma 5.91** (OrSubM). *If* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_3$*, and* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_4$*, then* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \vee T_2 <: T_3 \vee T_4$*.*

*Proof.* By (ST$^{\mathrm{m}}_{\#}$-Or1), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_3 \vee T_4$, by (ST$^{\mathrm{m}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_3 \vee T_4$. By (ST$^{\mathrm{m}}_{\#}$-Or2), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_4 <: T_3 \vee T_4$, by (ST$^{\mathrm{m}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_2 <: T_3 \vee T_4$. By (ST$^{\mathrm{m}}_{\#}$-Or), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 \vee T_2 <: T_3 \vee T_4$. □

**Lemma 5.92** (SRedSub). *If* $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\oplus} T_2$*, then* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_1 <: T_2$*. If* $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\ominus} T_2$*, then* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_2 <: T_1$*.*

*Idea.* $\vdash\!\longmapsto^{\mathrm{s}}_{\delta}$ implies subtyping in the direction of $\delta$ ▽

*Proof idea.* Straightforward induction ▽

*Proof.* Induction on $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_2$:

- Case (TR$^{\mathrm{s}}$-Refl): By (ST$^{\mathrm{s}}_{\#}$-Refl).
- Case (TR$^{\mathrm{s}}$-SelU): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_3..T_4\}$, and $\mathrm{F} \vdash [x_2/r]T_4 \longmapsto^{\mathrm{s}}_{\oplus} T_2$, and $\delta = \oplus$. By induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} [x_2/r]T_4 <: T_2$. By (ST$^{\mathrm{s}}_{\#}$-SelU), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} v_1.B(x_2) <: [x_2/r]T_4$. By (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} v_1.B(x_2) <: T_2$.
- Case (TR$^{\mathrm{s}}$-SelL): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_3..T_4\}$, and $\mathrm{F} \vdash [x_2/r]T_3 \longmapsto^{\mathrm{s}}_{\ominus} T_2$, and $\delta = \ominus$. By induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_2 <: [v_2/r]T_3$. By (ST$^{\mathrm{s}}_{\#}$-SelL), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} [x_2/r]T_3 <: v_1.B(x_2)$. By (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_2 <: v_1.B(x_2)$.
- Case (TR$^{\mathrm{s}}$-And): $T_1 = T_3 \wedge T_4$, and $T_2 = T_5 \wedge T_6$, where $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. If $\delta = \oplus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_3 <: T_5$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_4 <: T_6$. By 5.88(AndSubS), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_3 \wedge T_4 <: T_5 \wedge T_6$. If $\delta = \ominus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_5 <: T_3$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_6 <: T_4$. By 5.88(AndSubS), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_5 \wedge T_6 <: T_3 \wedge T_4$.
- Case (TR$^{\mathrm{s}}$-Or): $T_1 = T_3 \vee T_4$, and $T_2 = T_5 \vee T_6$, where $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. If $\delta = \oplus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_3 <: T_5$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_4 <: T_6$. By 5.89(OrSubS), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_3 \vee T_4 <: T_5 \vee T_6$. If $\delta = \ominus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_5 <: T_3$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_6 <: T_4$. By 5.89(OrSubS), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_5 \vee T_6 <: T_3 \vee T_4$.
- Case (TR$^{\mathrm{s}}$-Fld): $T_1 = \{a : T_3..T_4\}$, and $T_2 = \{a : T_5..T_6\}$, where $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{-\delta} T_5$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. If $\delta = \oplus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_4 <: T_6$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_5 <: T_3$. By (ST$^{\mathrm{s}}_{\#}$-Fld), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} \{a : T_3..T_4\} <: \{a : T_5..T_6\}$. If $\delta = \ominus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_3 <: T_5$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_6 <: T_4$. By (ST$^{\mathrm{s}}_{\#}$-Fld), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} \{a : T_5..T_6\} <: \{a : T_3..T_4\}$.
- Case (TR$^{\mathrm{s}}$-Typ): $T_1 = \{B(r) : T_3..T_4\}$, and $T_2 = \{B(r) : T_5..T_6\}$, where $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{-\delta} T_5$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. If $\delta = \oplus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_5 <: T_3$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_4 <: T_6$. By (ST$^{\mathrm{s}}_{\#}$-Typ), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} \{B(r) : T_3..T_4\} <: \{B(r) : T_5..T_6\}$. If $\delta = \ominus$, then by induction, $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_3 <: T_5$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_6 <: T_4$. By (ST$^{\mathrm{s}}_{\#}$-Typ), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} \{B(r) : T_5..T_6\} <: \{B(r) : T_3..T_4\}$.

□

**Lemma 5.93** (SRedInv). *If* $\mathrm{F} \vdash T_2 \wedge T_3 \longmapsto^{\mathrm{s}}_{\delta} T_1$*, then there exist* $T_4$*,* $T_5$*, such that* $T_1 = T_4 \wedge T_5$*, and* $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4$*, and* $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$*. If* $\mathrm{F} \vdash T_2 \vee T_3 \longmapsto^{\mathrm{s}}_{\delta} T_1$*, then there exist* $T_4$*,* $T_5$*, such that* $T_1 = T_4 \vee T_5$*, and* $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4$*, and* $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$*. If* $\mathrm{F} \vdash \{a : T_2..T_3\} \longmapsto^{\mathrm{s}}_{\delta} T_1$*, then there exist* $T_4$*,* $T_5$*, such that* $T_1 = \{a : T_4..T_5\}$*, and* $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{-\delta} T_4$*, and* $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$*. If* $\mathrm{F} \vdash \{B(r) : T_2..T_3\} \longmapsto^{\mathrm{s}}_{\delta} T_1$*, then there exist* $T_4$*,* $T_5$*, such that* $T_1 = \{B(r) : T_4..T_5\}$*, and* $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{-\delta} T_4$*, and* $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$*.*

*Idea.* For the purpose of induction or inversion of $\vdash\longmapsto^{\mathrm{s}}_{\delta}$ in the case of intersection, union, field and type member types, we can assume the relation between the corresponding parts. If the (TR$^{\mathrm{s}}$-Refl) rule was used, the situation is the same as if the specific rule was used. ▽

*Proof.*

- $T_2 \wedge T_3$: By inversion: Subcase (TR$^{\mathrm{s}}$-Refl): $T_1 = T_2 \wedge T_3$. Choose $T_4 = T_2$, and $T_5 = T_3$. By (TR$^{\mathrm{s}}$-Refl). Subcase (TR$^{\mathrm{s}}$-And): Trivially.
- $T_2 \vee T_3$: By inversion: Subcase (TR$^{\mathrm{s}}$-Refl): $T_1 = T_2 \vee T_3$. Choose $T_4 = T_2$, and $T_5 = T_3$. By (TR$^{\mathrm{s}}$-Refl). Subcase (TR$^{\mathrm{s}}$-Or): Trivially.
- $\{a : T_2..T_3\}$: By inversion: Subcase (TR$^{\mathrm{s}}$-Refl): $T_1 = \{a : T_2..T_3\}$. Choose $T_4 = T_2$, and $T_5 = T_3$. By (TR$^{\mathrm{s}}$-Refl). Subcase (TR$^{\mathrm{s}}$-Fld): Trivially.
- $\{B(r) : T_2..T_3\}$: By inversion: Subcase (TR$^{\mathrm{s}}$-Refl): $T_1 = \{B(r) : T_2..T_3\}$. Choose $T_4 = T_2$, and $T_5 = T_3$. By (TR$^{\mathrm{s}}$-Refl). Subcase (TR$^{\mathrm{s}}$-Typ): Trivially.

□

**Lemma 5.94** (SRedMut). *If* $\mathrm{F} \vdash \{\mathsf{M}(r_0) : \bot..\bot\} \longmapsto^{\mathrm{s}}_{\delta} T_2$*, then* $T_2 = \{\mathsf{M}(r_0) : \bot..\bot\}$*.*

*Idea.* $\{\mathsf{M}(r_0) : \bot..\bot\}$ does not reduce to any other type. ▽

*Proof.* By inversion:

Case (TR$^{\mathrm{s}}$-Refl): Trivially.

Case (TR$^{\mathrm{s}}$-Typ): $T_2 = \{\mathsf{M}(r_0) : T_3..T_4\}$, where $\mathrm{F} \vdash \bot \longmapsto^{\mathrm{s}}_{-\delta} T_3$, and $\mathrm{F} \vdash \bot \longmapsto^{\mathrm{s}}_{\delta} T_4$. By 5.93(SRedInv), $T_3 = \bot$, and $T_4 = \bot$. □

**Lemma 5.95** (SRedTrans). *If* $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_2$*, and* $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_3$*, then* $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$*.*

*Idea.* $\vdash\longmapsto^{\mathrm{s}}_{\delta}$ is transitive ▽

*Proof.* Induction on $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_2$:

- Case (TR$^{\mathrm{s}}$-Refl): $T_1 = T_2$. Trivially.
- Case (TR$^{\mathrm{s}}$-SelU): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r) : T_4..T_5\}$, and $\mathrm{F} \vdash [x_2/r]T_5 \longmapsto^{\mathrm{s}}_{\oplus} T_2$. By induction, $\mathrm{F} \vdash [x_2/r]T_5 \longmapsto^{\mathrm{s}}_{\oplus} T_3$. By (TR$^{\mathrm{s}}$-SelU), $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\oplus} T_3$.
- Case (TR$^{\mathrm{s}}$-SelL): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r) : T_4..T_5\}$, and $\mathrm{F} \vdash [x_2/r]T_4 \longmapsto^{\mathrm{s}}_{\ominus} T_2$. By induction, $\mathrm{F} \vdash [x_2/r]T_4 \longmapsto^{\mathrm{s}}_{\ominus} T_3$. By (TR$^{\mathrm{s}}$-SelL), $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\ominus} T_3$.
- Case (TR$^{\mathrm{s}}$-And): $T_1 = T_4 \wedge T_5$, and $T_2 = T_6 \wedge T_7$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_7$. By 5.93(SRedInv), $T_3 = T_8 \wedge T_9$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_8$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By induction, $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By (TR$^{\mathrm{s}}$-And), $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$.
- Case (TR$^{\mathrm{s}}$-Or): $T_1 = T_4 \vee T_5$, and $T_2 = T_6 \vee T_7$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_7$. By 5.93(SRedInv), $T_3 = T_8 \vee T_9$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_8$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By induction, $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By (TR$^{\mathrm{s}}$-Or), $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$.
- Case (TR$^{\mathrm{s}}$-Fld): $T_1 = \{a : T_4..T_5\}$, and $T_2 = \{a : T_6..T_7\}$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{-\delta} T_6$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_7$. By 5.93(SRedInv), $T_3 = \{a : T_8..T_9\}$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{-\delta} T_8$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By induction, $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{-\delta} T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By (TR$^{\mathrm{s}}$-Fld), $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$.
- Case (TR$^{\mathrm{s}}$-Typ): $T_1 = \{B(r) : T_4..T_5\}$, and $T_2 = \{B(r) : T_6..T_7\}$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{-\delta} T_6$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_7$. By 5.93(SRedInv), $T_3 = \{B(r) : T_8..T_9\}$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{-\delta} T_8$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By induction, $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{-\delta} T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By (TR$^{\mathrm{s}}$-Typ), $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$.

□

**Lemma 5.96** (SRedCom). *If* $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_2$*, and* $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$*, then there exists* $T_4$*, such that* $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4$*, and* $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_4$*.*

*Idea.* If a type reduces to two types, then we can find a common type to which both of those type reduce. ▽

*Proof idea.* The reductions can differ, if on some part of the type, one used the (TR$^{\mathrm{s}}$-Refl) rule while the other uses the (TR$^{\mathrm{s}}$-SelU) or (TR$^{\mathrm{s}}$-SelL) rule. In that case, we always choose the selection rule. ▽

*Proof.* Induction on $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_2$:

- Case (TR$^{\mathrm{s}}$-Refl): $T_1 = T_2$. Choose $T_4 = T_3$. By (TR$^{\mathrm{s}}$-Refl).
- Case (TR$^{\mathrm{s}}$-SelU): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r) : T_5..T_6\}$, and $\mathrm{F} \vdash [x_2/r]T_6 \longmapsto^{\mathrm{s}}_{\oplus} T_2$, and $\delta = \oplus$. By inversion: Subcase (TR$^{\mathrm{s}}$-SelU): $\mathrm{F} \vdash_! v_1 : \{B(r) : T_7..T_8\}$, and $\mathrm{F} \vdash [x_2/r]T_8 \longmapsto^{\mathrm{s}}_{\oplus} T_2$. By 5.52(UPrecTyp), $T_6 = T_8$, therefore $\mathrm{F} \vdash [x_2/r]T_6 \longmapsto^{\mathrm{s}}_{\oplus} T_3$. By induction, exists $T_4$, such that $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\oplus} T_4$, and $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\oplus} T_4$. Subcase (TR$^{\mathrm{s}}$-Refl): $T_1 = T_3$. Choose $T_4 = T_2$.
- Case (TR$^{\mathrm{s}}$-SelL): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r) : T_5..T_6\}$, and $\mathrm{F} \vdash [x_2/r]T_5 \longmapsto^{\mathrm{s}}_{\ominus} T_2$, and $\delta = \ominus$. By inversion: Subcase (TR$^{\mathrm{s}}$-SelL), and $\mathrm{F} \vdash [x_2/r]T_5 \longmapsto^{\mathrm{s}}_{\ominus} T_3$: By induction, exists $T_4$, such that $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\ominus} T_4$, and $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\ominus} T_4$. Subcase (TR$^{\mathrm{s}}$-Refl): $T_1 = T_3$. Choose $T_4 = T_2$.
- Case (TR$^{\mathrm{s}}$-And): $T_1 = T_5 \wedge T_6$, and $T_2 = T_7 \wedge T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_8$. By 5.93(SRedInv), $T_3 = T_9 \wedge T_{10}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_9$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$. By induction, exists $T_{11}$, such that $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$. By induction, exists $T_{12}$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{12}$. By (TR$^{\mathrm{s}}$-And), $\mathrm{F} \vdash T_7 \wedge T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{11} \wedge T_{12}$. By (TR$^{\mathrm{s}}$-And), $\mathrm{F} \vdash T_9 \wedge T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{11} \wedge T_{12}$. Choose $T_4 = T_{11} \wedge T_{12}$.
- Case (TR$^{\mathrm{s}}$-Or): $T_1 = T_5 \vee T_6$, and $T_2 = T_7 \vee T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_8$. By 5.93(SRedInv), $T_3 = T_9 \vee T_{10}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{\delta} T_9$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$. By induction, exists $T_{11}$, such that $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$. By induction, exists $T_{12}$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{12}$. By (TR$^{\mathrm{s}}$-Or), $\mathrm{F} \vdash T_7 \vee T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{11} \vee T_{12}$. By (TR$^{\mathrm{s}}$-Or), $\mathrm{F} \vdash T_9 \vee T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{11} \vee T_{12}$. Choose $T_4 = T_{11} \vee T_{12}$.
- Case (TR$^{\mathrm{s}}$-Fld): $T_1 = \{a : T_5..T_6\}$, and $T_2 = \{a : T_7..T_8\}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{-\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_8$. By 5.93(SRedInv), $T_3 = \{a : T_9..T_{10}\}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{-\delta} T_9$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$. By induction, exists $T_{11}$, such that $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_{11}$, and $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{-\delta} T_{11}$. By induction, exists $T_{12}$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{12}$. By (TR$^{\mathrm{s}}$-Fld), $\mathrm{F} \vdash \{a : T_7..T_8\} \longmapsto^{\mathrm{s}}_{\delta} \{a : T_{11}..T_{12}\}$. By (TR$^{\mathrm{s}}$-Fld), $\mathrm{F} \vdash \{a : T_9..T_{10}\} \longmapsto^{\mathrm{s}}_{\delta} \{a : T_{11}..T_{12}\}$. Choose $T_4 = \{a : T_{11}..T_{12}\}$.
- Case (TR$^{\mathrm{s}}$-Typ): $T_1 = \{B(r) : T_5..T_6\}$, and $T_2 = \{B(r) : T_7..T_8\}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{-\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_8$. By 5.93(SRedInv), $T_3 = \{B(r) : T_9..T_{10}\}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{-\delta} T_9$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$. By induction, exists $T_{11}$, such that $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_{11}$, and $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{-\delta} T_{11}$. By induction, exists $T_{12}$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{12}$. By (TR$^{\mathrm{s}}$-Typ), $\mathrm{F} \vdash \{B(r) : T_7..T_8\} \longmapsto^{\mathrm{s}}_{\delta} \{B(r) : T_{11}..T_{12}\}$. By (TR$^{\mathrm{s}}$-Typ), $\mathrm{F} \vdash \{B(r) : T_9..T_{10}\} \longmapsto^{\mathrm{s}}_{\delta} \{B(r) : T_{11}..T_{12}\}$. Choose $T_4 = \{B(r) : T_{11}..T_{12}\}$.

□

**Lemma 5.97** (SRedEq). *If $\rho \vdash T_1 \approx T_2$, and $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$, then there exists $T_4$, such that $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4$, and $\rho \vdash T_3 \approx T_4$.*

*Idea.* S reduction preserves equivalence ▽

*Proof.* Induction on $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$:

- Case (TR$^{\mathrm{s}}$-Refl): $T_1 = T_3$. Choose $T_4 = T_2$. By (TR$^{\mathrm{s}}$-Refl), $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4$.
- Case (TR$^{\mathrm{s}}$-SelL): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r) : T_5..T_6\}$, and $\mathrm{F} \vdash [x_2/r]T_5 \longmapsto^{\mathrm{s}}_{\ominus} T_3$, and $\delta = \ominus$. By inversion:
  - Case (TE-Refl): $T_1 = T_2$. Choose $T_4 = T_3$. By (TE-Refl), $\rho \vdash T_3 \approx T_4$.
  - Case (TE-Sel): $T_2 = v_2.A(x_2)$, where $A = B$, and $\rho \vdash v_1 \approx v_2$. By 5.56(EqPrecTypG), $\mathrm{F} \vdash_! v_2 : \{B(r) : T_7..T_8\}$, where $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By 5.26(SubEq), $\rho \vdash [x_2/r]T_5 \approx [x_2/r]T_7$. By induction, exists $T_4$, such that $\mathrm{F} \vdash [x_2/r]T_7 \longmapsto^{\mathrm{s}}_{\ominus} T_4$, and $\rho \vdash T_3 \approx T_4$. By (TR$^{\mathrm{s}}$-SelL).
- Case (TR$^{\mathrm{s}}$-SelU): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_! v_1 : \{B(r) : T_5..T_6\}$, and $\mathrm{F} \vdash [x_2/r]T_6 \longmapsto^{\mathrm{s}}_{\oplus} T_3$, and $\delta = \oplus$. By inversion:

  - Case (TE-Refl): $T_1 = T_2$. Choose $T_4 = T_3$. By (TE-Refl), $\rho \vdash T_3 \approx T_4$.
  - Case (TE-Sel): $T_2 = v_2.A(x_2)$, where $A = B$, and $\rho \vdash v_1 \approx v_2$. By 5.56(EqPrecTypG), $\mathrm{F} \vdash_{!} v_2 : \{B(r) : T_7..T_8\}$, where $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By 5.26(SubEq), $\rho \vdash [x_2/r]T_6 \approx [x_2/r]T_8$. By induction, exists $T_4$, such that $\mathrm{F} \vdash [x_2/r]T_8 \longmapsto^{\mathsf{s}}_{\ominus} T_4$, and $\rho \vdash T_3 \approx T_4$. By (TR$^{\mathsf{s}}$-SelU).

- Case (TR$^{\mathsf{s}}$-And): $T_1 = T_5 \wedge T_6$, and $T_3 = T_7 \wedge T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathsf{s}}_{\delta} T_8$. By 5.4(TEInv), $T_3 = T_9 \wedge T_{10}$, where $\rho \vdash T_5 \approx T_9$, and $\rho \vdash T_6 \approx T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathsf{s}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \wedge T_{12}$. By (TE-And) and (TR$^{\mathsf{s}}$-And).
- Case (TR$^{\mathsf{s}}$-Or): $T_1 = T_5 \vee T_6$, and $T_3 = T_7 \vee T_8$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathsf{s}}_{\delta} T_8$. By 5.4(TEInv), $T_3 = T_9 \vee T_{10}$, where $\rho \vdash T_5 \approx T_9$, and $\rho \vdash T_6 \approx T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathsf{s}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \vee T_{12}$. By (TE-Or) and (TR$^{\mathsf{s}}$-Or).
- Case (TR$^{\mathsf{s}}$-Fld): $T_1 = \{a : T_5..T_6\}$, and $T_3 = \{a : T_7..T_8\}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathsf{s}}_{\delta} T_8$. By 5.4(TEInv), $T_3 = \{a : T_9..T_{10}\}$, where $\rho \vdash T_5 \approx T_9$, and $\rho \vdash T_6 \approx T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathsf{s}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = \{a : T_{11}..T_{12}\}$. By (TE-Fld) and (TR$^{\mathsf{s}}$-Fld).
- Case (TR$^{\mathsf{s}}$-Typ): $T_1 = \{B(r) : T_5..T_6\}$, and $T_3 = \{B(r) : T_7..T_8\}$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathsf{s}}_{\delta} T_8$. By 5.4(TEInv), $T_3 = \{B(r) : T_9..T_{10}\}$, where $\rho \vdash T_5 \approx T_9$, and $\rho \vdash T_6 \approx T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathsf{s}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = \{B(r) : T_{11}..T_{12}\}$. By (TE-Typ) and (TR$^{\mathsf{s}}$-Typ).

□

**Lemma 5.98** (SRedSubCom). *If* $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_2$, *and* $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_3$, *and* $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_4$, *then there exist* $T_5$, $T_6$, *such that* $\mathrm{F} \vdash T_3 \longmapsto^{\mathsf{s}}_{\delta} T_5$, *and* $\mathrm{F} \vdash T_4 \longmapsto^{\mathsf{s}}_{\delta} T_6$, *and* $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_5 <: T_6$.

*Idea.* If we have subtyping of $T_1$ and $T_2$, which uses selection subtyping only in one direction, in an inert context, and if we reduce the types on both sides by inlining some type selections in the same direction, then we can further reduce those to again have subtyping between them. (Method types are overlooked in this phase.) ▽

*Proof.* Induction on $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_2$:

- Case (ST$^{\mathsf{s}}_{\#}$-Top): $T_2 = \top$. By inversion of (TR$^{\mathsf{s}}$-Refl), $T_4 = \top$. Choose $T_5 = T_3$, and $T_6 = \top$. By (ST$^{\mathsf{s}}_{\#}$-Top), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_5 <: T_6$. By (TR$^{\mathsf{s}}$-Refl).
- Case (ST$^{\mathsf{s}}_{\#}$-Bot): $T_1 = \bot$. By inversion of (TR$^{\mathsf{s}}$-Refl), $T_3 = \bot$. Choose $T_5 = \bot$, and $T_6 = T_4$. By (ST$^{\mathsf{s}}_{\#}$-Bot) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$^{\mathsf{s}}_{\#}$-Refl): $T_1 = T_2$. By 5.96(SRedCom), exists $T_5$, such that $\mathrm{F} \vdash T_3 \longmapsto^{\mathsf{s}}_{\delta} T_5$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathsf{s}}_{\delta} T_5$. Choose $T_6 = T_5$. By (ST$^{\mathsf{s}}_{\#}$-Refl).
- Case (ST$^{\mathsf{s}}_{\#}$-N-Rec): $T_1 = \mathsf{N}$, and $T_2 = \mu(s : T_7)$. By inversion of (TR$^{\mathsf{s}}$-Refl), $T_3 = T_1$, and $T_4 = T_2$. Choose $T_5 = T_3$, and $T_6 = T_4$.
- Case (ST$^{\mathsf{s}}_{\#}$-N-M): $T_1 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_2 = \bot$. By 5.93(SRedInv), $T_3 = T_8 \wedge T_9$, where $\mathrm{F} \vdash \mathsf{N} \longmapsto^{\mathsf{s}}_{\delta} T_8$, and $\mathrm{F} \vdash \{\mathsf{M}(r_0) : \bot..\bot\} \longmapsto^{\mathsf{s}}_{\delta} T_9$. By inversion of (TR$^{\mathsf{s}}$-Refl), $T_8 = \mathsf{N}$. By 5.94(SRedMut), $T_9 = \{\mathsf{M}(r_0) : \bot..\bot\}$, therefore $T_3 = T_1$. By inversion of (TR$^{\mathsf{s}}$-Refl), $T_4 = T_2$. Choose $T_5 = T_3$, and $T_6 = T_4$.
- Case (ST$^{\mathsf{s}}_{\#}$-And1): $T_1 = T_2 \wedge T_7$. By 5.93(SRedInv), $T_3 = T_8 \wedge T_9$, where $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_8$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathsf{s}}_{\delta} T_9$. By 5.96(SRedCom), exists $T_6$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathsf{s}}_{\delta} T_6$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathsf{s}}_{\delta} T_6$. Choose $T_5 = T_6 \wedge T_9$. By (ST$^{\mathsf{s}}_{\#}$-And1), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_5 <: T_6$. By (TR$^{\mathsf{s}}$-Refl), $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_9$. By (TR$^{\mathsf{s}}$-And), $\mathrm{F} \vdash T_3 \longmapsto^{\mathsf{s}}_{\delta} T_5$.
- Case (ST$^{\mathsf{s}}_{\#}$-And2): $T_1 = T_7 \wedge T_2$. By 5.93(SRedInv), $T_3 = T_9 \wedge T_8$, where $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_8$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathsf{s}}_{\delta} T_9$. By 5.96(SRedCom), exists $T_6$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathsf{s}}_{\delta} T_6$, and $\mathrm{F} \vdash T_4 \longmapsto^{\mathsf{s}}_{\delta} T_6$. Choose $T_5 = T_9 \wedge T_6$. By (ST$^{\mathsf{s}}_{\#}$-And2), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_5 <: T_6$. By (TR$^{\mathsf{s}}$-Refl), $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_9$. By (TR$^{\mathsf{s}}$-And), $\mathrm{F} \vdash T_3 \longmapsto^{\mathsf{s}}_{\delta} T_5$.
- Case (ST$^{\mathsf{s}}_{\#}$-And): $T_2 = T_7 \wedge T_8$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_8$. By 5.93(SRedInv), $T_4 = T_9 \wedge T_{10}$, where $\mathrm{F} \vdash T_7 \longmapsto^{\mathsf{s}}_{\delta} T_9$, and $\mathrm{F} \vdash T_8 \longmapsto^{\mathsf{s}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{13}$, such that $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_{11} <: T_{13}$, and $\mathrm{F} \vdash T_3 \longmapsto^{\mathsf{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_{13}$. By induction, exist $T_{12}$, $T_{14}$, such that $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_{12} <: T_{14}$, and $\mathrm{F} \vdash T_3 \longmapsto^{\mathsf{s}}_{\delta} T_{12}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathsf{s}}_{\delta} T_{14}$.

  - If $\delta = \oplus$. By 5.92(SRedSub), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_3 <: T_{11}$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_3 <: T_{12}$. Choose $T_5 = T_3$. By (TR$^{\mathrm{s}}$-Refl), F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$.
  - Otherwise, $\delta = \ominus$. By 5.96(SRedCom), exists $T_5$, such that F $\vdash T_{11} \longmapsto^{\mathrm{s}}_{\delta} T_5$, and F $\vdash T_{12} \longmapsto^{\mathrm{s}}_{\delta} T_5$. By 5.95(SRedTrans), F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$. By 5.92(SRedSub), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_{11}$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_{12}$.

  Choose $T_6 = T_{13} \wedge T_{14}$. By (ST$^{\mathrm{s}}_{\#}$-Trans), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_{13}$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_{14}$. By (ST$^{\mathrm{s}}_{\#}$-And), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-Or1): $T_2 = T_1 \vee T_7$. By 5.93(SRedInv), $T_4 = T_8 \vee T_9$, where F $\vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_8$, and F $\vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By 5.96(SRedCom), exists $T_5$, such that F $\vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$. Choose $T_6 = T_5 \vee T_9$. By (ST$^{\mathrm{s}}_{\#}$-Or1), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$. By (TR$^{\mathrm{s}}$-Refl), F $\vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By (TR$^{\mathrm{s}}$-Or), F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-Or2): $T_2 = T_7 \vee T_1$. By 5.93(SRedInv), $T_4 = T_9 \vee T_8$, where F $\vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_8$, and F $\vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By 5.96(SRedCom), exists $T_5$, such that F $\vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$. Choose $T_6 = T_9 \vee T_5$. By (ST$^{\mathrm{s}}_{\#}$-Or2), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$. By (TR$^{\mathrm{s}}$-Refl), F $\vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By (TR$^{\mathrm{s}}$-Or), F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-Or): $T_1 = T_7 \vee T_8$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_7 <: T_2$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_8 <: T_2$. By 5.93(SRedInv), $T_3 = T_9 \vee T_{10}$, where F $\vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$, and F $\vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$. By induction, exist $T_{11}, T_{13}$, such that F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{11} <: T_{13}$, and F $\vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$, and F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_{13}$. By induction, exist $T_{12}, T_{14}$, such that F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{12} <: T_{14}$, and F $\vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_{14}$.

  - If $\delta = \ominus$. By 5.92(SRedSub), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{13} <: T_4$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{14} <: T_4$. Choose $T_6 = T_4$. By (TR$^{\mathrm{s}}$-Refl), F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$.
  - Otherwise, $\delta = \oplus$. By 5.96(SRedCom), exists $T_6$, such that F $\vdash T_{13} \longmapsto^{\mathrm{s}}_{\delta} T_6$, and F $\vdash T_{14} \longmapsto^{\mathrm{s}}_{\delta} T_6$. By 5.95(SRedTrans), F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. By 5.92(SRedSub), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{13} <: T_6$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{14} <: T_6$.

  Choose $T_5 = T_{11} \vee T_{12}$. By (ST$^{\mathrm{s}}_{\#}$-Trans), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{11} <: T_6$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{12} <: T_6$. By (ST$^{\mathrm{s}}_{\#}$-Or), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-Trans): F;$\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_7$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_7 <: T_2$. By (TR$^{\mathrm{s}}$-Refl), F $\vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_7$.

  - If $\delta = \oplus$. By induction, exist $T_5, T_9$, such that F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_9$, and F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and F $\vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By induction, exist $T_{10}, T_6$, such that F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{10} <: T_6$, and F $\vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$, and F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. By 5.92(SRedSub), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_9 <: T_{10}$. By (ST$^{\mathrm{s}}_{\#}$-Trans), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.
  - Otherwise, $\delta = \ominus$. By induction, exist $T_9, T_6$, such that F;$\rho \vdash^{\mathrm{s}}_{\delta} T_9 <: T_6$, and F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$, and F $\vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_9$. By induction, exist $T_5, T_{10}$, such that F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_{10}$, and F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and F $\vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$. By 5.92(SRedSub), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{10} <: T_9$. By (ST$^{\mathrm{s}}_{\#}$-Trans), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-SelL): $T_2 = v_1.B(x_2)$, and F $\vdash_! v_1 : \{B(r) : T_7..T_8\}$, and $T_1 = [x_2/r]T_7$, and $\delta = \ominus$. By (TR$^{\mathrm{s}}$-SelL), F $\vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_3$. By 5.96(SRedCom), exists $T_6$, such that F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_6$, and F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. Choose $T_5 = T_6$. By (ST$^{\mathrm{s}}_{\#}$-Refl), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-SelU): $T_1 = v_1.B(x_2)$, and F $\vdash_! v_1 : \{B(r) : T_7..T_8\}$, and $T_2 = [x_2/r]T_8$, and $\delta = \oplus$. By (TR$^{\mathrm{s}}$-SelU), F $\vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_4$. By 5.96(SRedCom), exists $T_5$, and F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_5$. Choose $T_6 = T_5$. By (ST$^{\mathrm{s}}_{\#}$-Refl), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-Typ): $T_1 = \{B(r) : T_7..T_8\}$, and $T_2 = \{B(r) : T_9..T_{10}\}$, and F;$\rho \vdash^{\mathrm{s}}_{-\delta} T_9 <: T_7$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_8 <: T_{10}$. By 5.93(SRedInv), exist $T_{11}, T_{12}$, such that $T_3 = \{B(r) : T_{11}..T_{12}\}$, and F $\vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_{11}$, and F $\vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$. By 5.93(SRedInv), exist $T_{13}, T_{14}$, such that $T_4 = \{B(r) : T_{13}..T_{14}\}$, and F $\vdash T_9 \longmapsto^{\mathrm{s}}_{-\delta} T_{13}$, and F $\vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{14}$. By induction, exist $T_{15}, T_{17}$, and F $\vdash T_{11} \longmapsto^{\mathrm{s}}_{-\delta} T_{15}$, and F $\vdash T_{13} \longmapsto^{\mathrm{s}}_{-\delta} T_{17}$, and F;$\rho \vdash^{\mathrm{s}}_{-\delta} T_{17} <: T_{15}$. By induction, exist $T_{16}, T_{18}$, and F $\vdash T_{12} \longmapsto^{\mathrm{s}}_{\delta} T_{16}$, and F $\vdash T_{14} \longmapsto^{\mathrm{s}}_{\delta} T_{18}$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_{16} <: T_{18}$. Choose $T_5 = \{B(r) : T_{15}..T_{16}\}$, and $T_6 = \{B(r) : T_{17}..T_{18}\}$. By (ST$^{\mathrm{s}}_{\#}$-Typ), F;$\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$. By (TR$^{\mathrm{s}}$-Typ), F $\vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$. By (TR$^{\mathrm{s}}$-Typ), F $\vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-Fld): $T_1 = \{a : T_7..T_8\}$, and $T_2 = \{a : T_9..T_{10}\}$, and F;$\rho \vdash^{\mathrm{s}}_{-\delta} T_9 <: T_7$, and F;$\rho \vdash^{\mathrm{s}}_{\delta} T_8 <: T_{10}$. By 5.93(SRedInv), exist $T_{11}, T_{12}$, such that $T_3 = \{a : T_{11}..T_{12}\}$, and F $\vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_{11}$, and F $\vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$. By 5.93(SRedInv), exist $T_{13}, T_{14}$, such that $T_4 = \{a : T_{13}..T_{14}\}$, and F $\vdash T_9 \longmapsto^{\mathrm{s}}_{-\delta} T_{13}$,

and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{14}$. By induction, exist $T_{15}$, $T_{17}$, and $\mathrm{F} \vdash T_{11} \longmapsto^{\mathrm{s}}_{-\delta} T_{15}$, and $\mathrm{F} \vdash T_{13} \longmapsto^{\mathrm{s}}_{-\delta} T_{17}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{-\delta} T_{17} <: T_{15}$. By induction, exist $T_{16}$, $T_{18}$, and $\mathrm{F} \vdash T_{12} \longmapsto^{\mathrm{s}}_{\delta} T_{16}$, and $\mathrm{F} \vdash T_{14} \longmapsto^{\mathrm{s}}_{\delta} T_{18}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_{16} <: T_{18}$. Choose $T_5 = \{a : T_{15}..T_{16}\}$, and $T_6 = \{a : T_{17}..T_{18}\}$. By (ST$^{\mathrm{s}}_{\#}$-Fld), F; $\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$. By (TR$^{\mathrm{s}}$-Fld), $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$. By (TR$^{\mathrm{s}}$-Fld), $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-Met): $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, and $T_2 = \{m(z : T_{10}, r : T_{12}) : T_{11}\}$. By inversion of (TR$^{\mathrm{s}}$-Refl), $T_3 = T_1$, and $T_4 = T_2$. Choose $T_5 = T_3$, and $T_6 = T_4$.
- Case (ST$^{\mathrm{s}}_{\#}$-TypAnd): $T_1 = \{B(r) : T_7..T_8\} \wedge \{B(r) : T_9..T_{10}\}$, and $T_2 = \{B(r) : T_7 \vee T_9..T_8 \wedge T_{10}\}$. By 5.93(SRedInv), $T_3 = \{B(r) : T_{11}..T_{12}\} \wedge \{B(r) : T_{13}..T_{14}\}$, where $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_{11}$, where $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, where $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{-\delta} T_{13}$, where $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{14}$, and $T_4 = \{B(r) : T_{15} \vee T_{17}..T_{16} \wedge T_{18}\}$, where $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_{15}$, where $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{16}$, where $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{-\delta} T_{17}$, where $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{18}$. By 5.96(SRedCom), exist $T_{19}$, $T_{20}$, $T_{21}$, $T_{22}$, such that $\mathrm{F} \vdash T_{11} \longmapsto^{\mathrm{s}}_{-\delta} T_{19}$, and $\mathrm{F} \vdash T_{15} \longmapsto^{\mathrm{s}}_{-\delta} T_{19}$, and $\mathrm{F} \vdash T_{12} \longmapsto^{\mathrm{s}}_{\delta} T_{20}$, and $\mathrm{F} \vdash T_{16} \longmapsto^{\mathrm{s}}_{\delta} T_{20}$, and $\mathrm{F} \vdash T_{13} \longmapsto^{\mathrm{s}}_{-\delta} T_{21}$, and $\mathrm{F} \vdash T_{17} \longmapsto^{\mathrm{s}}_{-\delta} T_{21}$, and $\mathrm{F} \vdash T_{14} \longmapsto^{\mathrm{s}}_{\delta} T_{22}$, and $\mathrm{F} \vdash T_{18} \longmapsto^{\mathrm{s}}_{\delta} T_{22}$. Choose $T_5 = \{B(r) : T_{19}..T_{20}\} \wedge \{B(r) : T_{21}..T_{22}\}$, and $T_6 = \{B(r) : T_{19} \vee T_{21}..T_{20} \wedge T_{22}\}$. By (TR$^{\mathrm{s}}$-Typ) and (TR$^{\mathrm{s}}$-And), $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$. By (TR$^{\mathrm{s}}$-And) and (TR$^{\mathrm{s}}$-Or) and (TR$^{\mathrm{s}}$-Typ), $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. By (ST$^{\mathrm{s}}_{\#}$-TypAnd), F; $\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-Eq): $\rho \vdash T_1 \approx T_2$.
  - If $\delta = \oplus$. By 5.97(SRedEq), exists $T_7$, such that $\rho \vdash T_3 \approx T_7$, and $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_7$. By 5.96(SRedCom), exists $T_6$, such that $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_6$. Choose $T_5 = T_3$. By (ST$^{\mathrm{s}}_{\#}$-Eq), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_3 <: T_7$. By 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_7 <: T_6$. By (ST$^{\mathrm{s}}_{\#}$-Trans), F; $\rho \vdash^{\mathrm{s}}_{\delta} T_3 <: T_6$.
  - Otherwise, $\delta = \ominus$. By 5.97(SRedEq), exists $T_7$, such that $\rho \vdash T_4 \approx T_7$, and $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_7$. By 5.96(SRedCom), exists $T_5$, such that $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_5$. Choose $T_6 = T_4$. By 5.2(EqSymm), $\rho \vdash T_7 \approx T_4$. By (ST$^{\mathrm{s}}_{\#}$-Eq), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_7 <: T_4$. By 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_7$. By (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_4$.
- Case (ST$^{\mathrm{s}}_{\#}$-N-Fld): $T_1 = \mathsf{N}$, and $T_2 = \{a : T_7..T_8\}$. By inversion of (TR$^{\mathrm{s}}$-Refl), $T_3 = T_1$. By 5.93(SRedInv), exist $T_{11}$, $T_{12}$, such that $T_4 = \{a : T_{11}..T_{12}\}$. Choose $T_5 = T_3$, and $T_6 = T_4$. By (ST$^{\mathrm{s}}_{\#}$-N-Fld), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-N-Met): $T_1 = \mathsf{N}$, and $T_2 = \{m(z : T_{10}, r : T_{12}) : T_{11}\}$. By inversion of (TR$^{\mathrm{s}}$-Refl), $T_3 = T_1$, and $T_4 = T_2$. Choose $T_5 = T_3$, and $T_6 = T_4$.
- Case (ST$^{\mathrm{s}}_{\#}$-N-Typ): $T_1 = \mathsf{N}$, and $T_2 = \{A(r) : T_7..T_8\}$. By inversion of (TR$^{\mathrm{s}}$-Refl), $T_3 = T_1$. By 5.93(SRedInv), exist $T_{11}$, $T_{12}$, such that $T_4 = \{A(r) : T_{11}..T_{12}\}$. Choose $T_5 = T_3$, and $T_6 = T_4$. By (ST$^{\mathrm{s}}_{\#}$-N-Typ), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-Dist): $T_1 = T_7 \wedge T_8 \vee T_9$. $T_2 = (T_7 \wedge T_8) \vee (T_7 \wedge T_9)$. By 5.93(SRedInv), $T_3 = T_{10} \wedge T_{11} \vee T_{12}$, where $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_{10}$, where $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$, where $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and $T_4 = (T_{13} \wedge T_{14}) \vee (T_{15} \wedge T_{16})$, where $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_{13}$, where $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{14}$, where $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_{15}$, where $\mathrm{F} \vdash T_9 \longmapsto^{\mathrm{s}}_{\delta} T_{16}$. By 5.96(SRedCom), exist $T_{17}$, $T_{18}$, $T_{19}$, such that $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{17}$, and $\mathrm{F} \vdash T_{13} \longmapsto^{\mathrm{s}}_{\delta} T_{17}$, and $\mathrm{F} \vdash T_{11} \longmapsto^{\mathrm{s}}_{\delta} T_{18}$, and $\mathrm{F} \vdash T_{14} \longmapsto^{\mathrm{s}}_{\delta} T_{18}$, and $\mathrm{F} \vdash T_{12} \longmapsto^{\mathrm{s}}_{\delta} T_{19}$, and $\mathrm{F} \vdash T_{16} \longmapsto^{\mathrm{s}}_{\delta} T_{19}$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{\delta} T_{17}$. By 5.96(SRedCom), exists $T_{20}$, such that $\mathrm{F} \vdash T_{15} \longmapsto^{\mathrm{s}}_{\delta} T_{20}$, and $\mathrm{F} \vdash T_{17} \longmapsto^{\mathrm{s}}_{\delta} T_{20}$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_{13} \longmapsto^{\mathrm{s}}_{\delta} T_{20}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathrm{s}}_{\delta} T_{20}$. Choose $T_5 = T_{20} \wedge T_{18} \vee T_{19}$, and $T_6 = (T_{20} \wedge T_{18}) \vee (T_{20} \wedge T_{19})$. By (TR$^{\mathrm{s}}$-Or) and (TR$^{\mathrm{s}}$-And), $\mathrm{F} \vdash T_3 \longmapsto^{\mathrm{s}}_{\delta} T_5$. By (TR$^{\mathrm{s}}$-And) and (TR$^{\mathrm{s}}$-Or), $\mathrm{F} \vdash T_4 \longmapsto^{\mathrm{s}}_{\delta} T_6$. By (ST$^{\mathrm{s}}_{\#}$-Dist), F; $\rho \vdash^{\mathrm{s}}_{\delta} T_5 <: T_6$.

□

**Lemma 5.99** (ToSRed)**.** *If* $\mathrm{F};\rho \vdash_{\#} T_1 <: T_2$, *and* $\delta \in \{\oplus, \oplus\}$, *then there exist* $T_3, T_4$, *such that* $\mathrm{F} \vdash T_1 \longmapsto^{\mathrm{s}}_{\delta} T_3$, *and* $\mathrm{F} \vdash T_2 \longmapsto^{\mathrm{s}}_{\delta} T_4$, *and* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_3 <: T_4$.

*Idea.* If we have subtyping of $T_1$ and $T_2$ in an inert context, then we can inline some type selections on both sides, such that the subtyping between the reduced types uses selection subtyping only in one direction. (Except in method types, which are overlooked in this phase.) ▽

*Proof.* Induction on $\mathrm{F};\rho \vdash_{\#} T_1 <: T_2$:

- Case (ST$_{\#}$-Top): $T_2 = \top$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathrm{s}}_{\#}$-Top) and (TR$^{\mathrm{s}}$-Refl).

- Case (ST$_{\#}$-Bot): $T_1 = \bot$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathsf{s}}_{\#}$-Bot) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-Refl): $T_1 = T_2$. Choose $T_3 = T_1$, and $T_4 = T_1$. By (ST$^{\mathsf{s}}_{\#}$-Refl) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-N-Rec): $T_1 = \mathsf{N}$, and $T_2 = \mu(s : T_5)$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathsf{s}}_{\#}$-N-Rec) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-N-M): $T_1 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_2 = \bot$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathsf{s}}_{\#}$-N-M) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-And1): $T_1 = T_2 \wedge T_5$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathsf{s}}_{\#}$-And1) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-And2): $T_1 = T_5 \wedge T_2$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathsf{s}}_{\#}$-And2) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-And): $T_2 = T_5 \wedge T_6$, and $\mathrm{F};\rho \vdash_{\#} T_1 <: T_5$, and $\mathrm{F};\rho \vdash_{\#} T_1 <: T_6$. By induction, there exist $T_7$, $T_8$, such that $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_8$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_7 <: T_8$. By induction, there exist $T_9$, $T_{10}$, such that $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_9$, and $\mathrm{F} \vdash T_6 \longmapsto^{\mathsf{s}}_{\delta} T_{10}$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_9 <: T_{10}$. Choose $T_4 = T_8 \wedge T_{10}$. By (TR$^{\mathsf{s}}$-And), $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_4$.

  - If $\delta = \oplus$, then by 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_9$. Choose $T_3 = T_1$. By (TR$^{\mathsf{s}}$-Refl), $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_3$.
  - Otherwise, $\delta = \ominus$. By 5.96(SRedCom), exists $T_3$, such that $\mathrm{F} \vdash T_7 \longmapsto^{\mathsf{s}}_{\delta} T_3$, and $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_3$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_3$. By 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_9$.

  By (ST$^{\mathsf{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_8$. By (ST$^{\mathsf{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_{10}$. By (ST$^{\mathsf{s}}_{\#}$-And), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_4$.
- Case (ST$_{\#}$-Or1): $T_2 = T_1 \vee T_5$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathsf{s}}_{\#}$-Or1) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-Or2): $T_2 = T_5 \vee T_1$. Choose $T_3 = T_1$, and $T_4 = T_2$. By (ST$^{\mathsf{s}}_{\#}$-Or2) and (TR$^{\mathsf{s}}$-Refl).
- Case (ST$_{\#}$-Or): $T_1 = T_5 \vee T_6$, and $\mathrm{F};\rho \vdash_{\#} T_5 <: T_2$, and $\mathrm{F};\rho \vdash_{\#} T_6 <: T_2$. By induction, there exist $T_7$, $T_8$, such that $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_8$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_7 <: T_8$. By induction, there exist $T_9$, $T_{10}$, such that $\mathrm{F} \vdash T_6 \longmapsto^{\mathsf{s}}_{\delta} T_9$, and $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_{10}$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_9 <: T_{10}$. Choose $T_3 = T_7 \vee T_9$. By (TR$^{\mathsf{s}}$-Or), $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_3$.

  - If $\delta = \ominus$, then by 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_8 <: T_2$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_{10} <: T_2$. Choose $T_4 = T_2$. By (TR$^{\mathsf{s}}$-Refl), $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_4$.
  - Otherwise, $\delta = \oplus$. By 5.96(SRedCom), exists $T_4$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathsf{s}}_{\delta} T_4$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathsf{s}}_{\delta} T_4$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_4$. By 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_8 <: T_4$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_{10} <: T_4$.

  By (ST$^{\mathsf{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_7 <: T_4$. By (ST$^{\mathsf{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_9 <: T_4$. By (ST$^{\mathsf{s}}_{\#}$-Or), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_4$.
- Case (ST$_{\#}$-Trans): $\mathrm{F};\rho \vdash_{\#} T_1 <: T_5$, and $\mathrm{F};\rho \vdash_{\#} T_5 <: T_2$. By induction, there exist $T_7$, $T_8$, such that $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_7$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_8$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_7 <: T_8$. By induction, there exist $T_9$, $T_{10}$, such that $\mathrm{F} \vdash T_5 \longmapsto^{\mathsf{s}}_{\delta} T_9$, and $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_{10}$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_9 <: T_{10}$. By 5.96(SRedCom), exists $T_{11}$, such that $\mathrm{F} \vdash T_8 \longmapsto^{\mathsf{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_{11}$.

  - If $\delta = \oplus$. By 5.98(SRedSubCom), exist $T_{12}$, $T_4$, such that $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_{12} <: T_4$, and $\mathrm{F} \vdash T_{11} \longmapsto^{\mathsf{s}}_{\delta} T_{12}$, and $\mathrm{F} \vdash T_{10} \longmapsto^{\mathsf{s}}_{\delta} T_4$. Choose $T_3 = T_7$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_2 \longmapsto^{\mathsf{s}}_{\delta} T_4$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_8 \longmapsto^{\mathsf{s}}_{\delta} T_{12}$. By 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_8 <: T_{12}$. By (ST$^{\mathsf{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By 5.98(SRedSubCom), exist $T_{12}$, $T_3$, such that $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_{12}$, and $\mathrm{F} \vdash T_7 \longmapsto^{\mathsf{s}}_{\delta} T_3$, and $\mathrm{F} \vdash T_{11} \longmapsto^{\mathsf{s}}_{\delta} T_{12}$. Choose $T_4 = T_{10}$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_1 \longmapsto^{\mathsf{s}}_{\delta} T_3$. By 5.95(SRedTrans), $\mathrm{F} \vdash T_9 \longmapsto^{\mathsf{s}}_{\delta} T_{12}$. By 5.92(SRedSub), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_{12} <: T_9$. By (ST$^{\mathsf{s}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_3 <: T_4$.
- Case (ST$_{\#}$-SelL): $T_2 = v_1.B(x_2)$, and $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_5..T_6\}$, and $T_1 = [x_2/r]T_5$. If $\delta = \oplus$, then by (TR$^{\mathsf{s}}$-Refl) and (TR$^{\mathsf{s}}$-SelU), $\mathrm{F} \vdash v_1.B(x_2) \longmapsto^{\mathsf{s}}_{\oplus} [x_2/r]T_6$. By 5.53(SubPrecTyp), $T_1 = \bot$, or $T_5 = T_6$. By (ST$^{\mathsf{s}}_{\#}$-Bot) or by (ST$^{\mathsf{s}}_{\#}$-Refl), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: [x_2/r]T_6$. Choose $T_3 = T_1$, and $T_4 = [x_2/r]T_6$. If $\delta = \ominus$, then by (TR$^{\mathsf{s}}$-Refl) and (TR$^{\mathsf{s}}$-SelL), $\mathrm{F} \vdash v_1.B(x_2) \longmapsto^{\mathsf{s}}_{\ominus} [x_2/r]T_5$. Choose $T_4 = T_3 = T_1$.
- Case (ST$_{\#}$-SelU): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_5..T_6\}$, and $T_2 = [x_2/r]T_6$. If $\delta = \oplus$, then by (TR$^{\mathsf{s}}$-Refl) and (TR$^{\mathsf{s}}$-SelU), $\mathrm{F} \vdash v_1.B(x_2) \longmapsto^{\mathsf{s}}_{\oplus} [x_2/r]T_6$. Choose $T_3 = T_4 = T_2$. If $\delta = \ominus$, then by (TR$^{\mathsf{s}}$-Refl) and (TR$^{\mathsf{s}}$-SelL), $\mathrm{F} \vdash v_1.B(x_2) \longmapsto^{\mathsf{s}}_{\ominus} [x_2/r]T_5$. By 5.53(SubPrecTyp), $T_5 = \bot$, or $T_5 = T_6$. By (ST$^{\mathsf{s}}_{\#}$-Bot) or by (ST$^{\mathsf{s}}_{\#}$-Refl), $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} [x_2/r]T_5 <: T_2$. Choose $T_3 = [x_2/r]T_5$, and $T_4 = T_2$.

- Case ($\mathrm{ST}_{\#}$-Typ): $T_1 = \{B(r) : T_5..T_6\}$, and $T_2 = \{B(r) : T_7..T_8\}$, and $\mathrm{F};\rho \vdash_{\#} T_7 <: T_5$, and $\mathrm{F};\rho \vdash_{\#} T_6 <: T_8$. By induction, there exist $T_9, T_{10}$, such that $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_9$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{-\delta} T_{10}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{-\delta} T_9 <: T_{10}$. By induction, there exist $T_{11}, T_{12}$, such that $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_{11} <: T_{12}$. By ($\mathrm{TR}^{\mathrm{s}}$-Typ), $\mathrm{F} \vdash \{B(r) : T_5..T_6\} \longmapsto^{\mathrm{s}}_{\delta} \{B(r) : T_{10}..T_{11}\}$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Typ), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} \{B(r) : T_{10}..T_{11}\} <: \{B(r) : T_9..T_{12}\}$. By ($\mathrm{TR}^{\mathrm{s}}$-Typ), $\mathrm{F} \vdash \{B(r) : T_7..T_8\} \longmapsto^{\mathrm{s}}_{\delta} \{B(r) : T_9..T_{12}\}$. Choose $T_3 = \{B(r) : T_{10}..T_{11}\}$, and $T_4 = \{B(r) : T_9..T_{12}\}$.
- Case ($\mathrm{ST}_{\#}$-Fld): $T_1 = \{a : T_5..T_6\}$, and $T_2 = \{a : T_7..T_8\}$, and $\mathrm{F};\rho \vdash_{\#} T_7 <: T_5$, and $\mathrm{F};\rho \vdash_{\#} T_6 <: T_8$. By induction, there exist $T_9$, $T_{10}$, such that $\mathrm{F} \vdash T_7 \longmapsto^{\mathrm{s}}_{-\delta} T_9$, and $\mathrm{F} \vdash T_5 \longmapsto^{\mathrm{s}}_{-\delta} T_{10}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{-\delta} T_9 <: T_{10}$. By induction, there exist $T_{11}, T_{12}$, such that $\mathrm{F} \vdash T_6 \longmapsto^{\mathrm{s}}_{\delta} T_{11}$, and $\mathrm{F} \vdash T_8 \longmapsto^{\mathrm{s}}_{\delta} T_{12}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_{11} <: T_{12}$. By ($\mathrm{TR}^{\mathrm{s}}$-Fld), $\mathrm{F} \vdash \{a : T_5..T_6\} \longmapsto^{\mathrm{s}}_{\delta} \{a : T_{10}..T_{11}\}$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Fld), $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} \{a : T_{10}..T_{11}\} <: \{a : T_9..T_{12}\}$. By ($\mathrm{TR}^{\mathrm{s}}$-Fld), $\mathrm{F} \vdash \{a : T_7..T_8\} \longmapsto^{\mathrm{s}}_{\delta} \{a : T_9..T_{12}\}$. Choose $T_3 = \{a : T_{10}..T_{11}\}$, and $T_4 = \{a : T_9..T_{12}\}$.
- Case ($\mathrm{ST}_{\#}$-Met): Choose $T_3 = T_1$, and $T_4 = T_2$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Met) and ($\mathrm{TR}^{\mathrm{s}}$-Refl).
- Case ($\mathrm{ST}_{\#}$-TypAnd): Choose $T_3 = T_1$, and $T_4 = T_2$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-TypAnd) and ($\mathrm{TR}^{\mathrm{s}}$-Refl).
- Case ($\mathrm{ST}_{\#}$-Eq): Choose $T_3 = T_1$, and $T_4 = T_2$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Eq) and ($\mathrm{TR}^{\mathrm{s}}$-Refl).
- Case ($\mathrm{ST}_{\#}$-N-Fld): Choose $T_3 = T_1$, and $T_4 = T_2$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-Fld) and ($\mathrm{TR}^{\mathrm{s}}$-Refl).
- Case ($\mathrm{ST}_{\#}$-N-Met): Choose $T_3 = T_1$, and $T_4 = T_2$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-Met) and ($\mathrm{TR}^{\mathrm{s}}$-Refl).
- Case ($\mathrm{ST}_{\#}$-N-Typ): Choose $T_3 = T_1$, and $T_4 = T_2$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-Typ) and ($\mathrm{TR}^{\mathrm{s}}$-Refl).
- Case ($\mathrm{ST}_{\#}$-Dist): Choose $T_3 = T_1$, and $T_4 = T_2$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Dist) and ($\mathrm{TR}^{\mathrm{s}}$-Refl).

□

**Lemma 5.100** (TRedMut). *If* $\{\mathsf{M}(r_0) : \bot..\bot\} \longmapsto^{\mathrm{m}}_{\oplus} T_2$*, then* $T_2 = \{\mathsf{M}(r_0) : \bot..\bot\}$.

*Proof.* By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Typ). $T_2 = \{\mathsf{M}(r_0) : T_3..T_4\}$, where $\bot \longmapsto^{\mathrm{e}}_{\ominus} T_3$, and $\bot \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Bot), $T_3 = \bot$, and $T_4 = \bot$. □

**Lemma 5.101** (ERedMut). *If* $\{\mathsf{M}(r_0) : \bot..\bot\} \longmapsto^{\mathrm{e}}_{\oplus} T_2$*, then* $T_2 = \{\mathsf{M}(r_0) : \bot..\bot\}$.

*Proof.* By inversion of (TER-Typ). $T_2 = \{\mathsf{M}(r_0) : T_3..T_4\}$, where $\bot \longmapsto^{\mathrm{e}}_{\ominus} T_3$, and $\bot \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By inversion of (TER-Bot), $T_3 = \bot$, and $T_4 = \bot$. □

**Lemma 5.102** (TRedEx). *For each* $T_1$ *there exist* $T_2, T_3$*, such that* $T_1 \longmapsto^{\mathrm{m}}_{\oplus} T_2$*, and* $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_3$.

*Idea.* In a type, we can replace occurrences of method types by $\top$ or $\bot$. Occurrences in recursive types are not touched. ▽

*Proof.*

- If $T_1 = \top$, then choose $T_2 = T_3 = \top$. By ($\mathrm{TR}^{\mathrm{m}}$-Top).
- If $T_1 = \bot$, then choose $T_2 = T_3 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-Bot).
- If $T_1 = \mathsf{N}$, then choose $T_2 = \mathsf{N}$, and $T_3 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-N) and ($\mathrm{TR}^{\mathrm{m}}$-N-Bot).
- If $T_1 = \mu(s : T_4)$, then choose $T_2 = T_3 = T_1$. By ($\mathrm{TR}^{\mathrm{m}}$-Rec).
- If $T_1 = x_1.B(x_2)$, then choose $T_2 = T_3 = T_1$. By ($\mathrm{TR}^{\mathrm{m}}$-Sel).
- If $T_1 = T_4 \wedge T_5$, then by induction, there exist $T_6, T_7, T_8, T_9$, such that $T_4 \longmapsto^{\mathrm{m}}_{\oplus} T_6$, and $T_5 \longmapsto^{\mathrm{m}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{m}}_{\ominus} T_8$, and $T_5 \longmapsto^{\mathrm{m}}_{\ominus} T_9$, then choose $T_2 = T_6 \wedge T_7$, and $T_3 = T_8 \wedge T_9$. By ($\mathrm{TR}^{\mathrm{m}}$-And).
- If $T_1 = T_4 \vee T_5$, then by induction, there exist $T_6, T_7, T_8, T_9$, such that $T_4 \longmapsto^{\mathrm{m}}_{\oplus} T_6$, and $T_5 \longmapsto^{\mathrm{m}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{m}}_{\ominus} T_8$, and $T_5 \longmapsto^{\mathrm{m}}_{\ominus} T_9$, then choose $T_2 = T_6 \vee T_7$, and $T_3 = T_8 \vee T_9$. By ($\mathrm{TR}^{\mathrm{m}}$-Or).
- If $T_1 = \{a : T_4..T_5\}$, then by induction, there exist $T_6$, $T_7$, $T_8$, $T_9$, such that $T_4 \longmapsto^{\mathrm{m}}_{\ominus} T_6$, and $T_5 \longmapsto^{\mathrm{m}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{m}}_{\oplus} T_8$, and $T_5 \longmapsto^{\mathrm{m}}_{\ominus} T_9$, then choose $T_2 = \{a : T_6..T_7\}$, and $T_3 = \{a : T_8..T_9\}$. By ($\mathrm{TR}^{\mathrm{m}}$-Fld).
- If $T_1 = \{B(r) : T_4..T_5\}$, then by induction, there exist $T_6$, $T_7$, $T_8$, $T_9$, such that $T_4 \longmapsto^{\mathrm{m}}_{\ominus} T_6$, and $T_5 \longmapsto^{\mathrm{m}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{m}}_{\oplus} T_8$, and $T_5 \longmapsto^{\mathrm{m}}_{\ominus} T_9$, then choose $T_2 = \{B(r) : T_6..T_7\}$, and $T_3 = \{B(r) : T_8..T_9\}$. By ($\mathrm{TR}^{\mathrm{m}}$-Typ).
- If $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, then choose $T_2 = \top$, and $T_3 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-MetU) and ($\mathrm{TR}^{\mathrm{m}}$-MetL).

□

**Lemma 5.103** (ERedEx). *For each $T_1$ there exist $T_2, T_3$, such that $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$, and $T_2$ **nosel** $y_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$, and $T_3$ **nosel** $y_2$.*

*Idea.* In a type, we can replace occurrences of method types and selections by $\top$ or $\bot$, such that the resulting type does not contain type selections. Occurrences in recursive types are not touched. ▽

*Proof.*

- If $T_1 = \top$, then choose $T_2 = T_3 = \top$. By (TER-Top) and (TN-Top).
- If $T_1 = \bot$, then choose $T_2 = T_3 = \bot$. By (TER-Bot) and (TN-Bot).
- If $T_1 = \mathsf{N}$, then choose $T_2 = \mathsf{N}$, and $T_3 = \bot$. By (TER-N) and (TN-N). By (TER-N-Bot) and (TN-Bot).
- If $T_1 = \mu(s : T_4)$, then choose $T_2 = T_3 = T_1$. By (TER-Rec) and (TN-Rec).
- If $T_1 = x_1.B(x_2)$, then choose $T_2 = \bot$, and $T_3 = \top$. By (TER-SelU), $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$. By (TER-SelL), $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$. By (TN-Bot), $T_2$ **nosel** $y_2$. By (TN-Top), $T_3$ **nosel** $y_2$.
- If $T_1 = T_4 \wedge T_5$, then by induction, there exist $T_6, T_7, T_8, T_9$, such that $T_4 \longmapsto^{\mathrm{e}}_{\oplus} T_6$, and $T_5 \longmapsto^{\mathrm{e}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{e}}_{\ominus} T_8$, and $T_5 \longmapsto^{\mathrm{e}}_{\ominus} T_9$, and $T_6$ **nosel** $y_2$, and $T_7$ **nosel** $y_2$, and $T_8$ **nosel** $y_2$, and $T_9$ **nosel** $y_2$, then choose $T_2 = T_6 \wedge T_7$, and $T_3 = T_8 \wedge T_9$. By (TR$^{\mathrm{m}}$-And), $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$. By (TN-And), $T_2$ **nosel** $y_2$, $T_3$ **nosel** $y_2$.
- If $T_1 = T_4 \vee T_5$, then by induction, there exist $T_6, T_7, T_8, T_9$, such that $T_4 \longmapsto^{\mathrm{e}}_{\oplus} T_6$, and $T_5 \longmapsto^{\mathrm{e}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{e}}_{\ominus} T_8$, and $T_5 \longmapsto^{\mathrm{e}}_{\ominus} T_9$, and $T_6$ **nosel** $y_2$, and $T_7$ **nosel** $y_2$, and $T_8$ **nosel** $y_2$, and $T_9$ **nosel** $y_2$, then choose $T_2 = T_6 \vee T_7$, and $T_3 = T_8 \vee T_9$. By (TR$^{\mathrm{m}}$-Or), $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$. By (TN-Or), $T_2$ **nosel** $y_2$, $T_3$ **nosel** $y_2$.
- If $T_1 = \{a : T_4..T_5\}$, then by induction, there exist $T_6$, $T_7$, $T_8$, $T_9$, such that $T_4 \longmapsto^{\mathrm{e}}_{\ominus} T_6$, and $T_5 \longmapsto^{\mathrm{e}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{e}}_{\oplus} T_8$, and $T_5 \longmapsto^{\mathrm{e}}_{\ominus} T_9$, and $T_6$ **nosel** $y_2$, and $T_7$ **nosel** $y_2$, and $T_8$ **nosel** $y_2$, and $T_9$ **nosel** $y_2$, then choose $T_2 = \{a : T_6..T_7\}$, and $T_3 = \{a : T_8..T_9\}$. By (TR$^{\mathrm{m}}$-Fld), $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$. By (TN-Fld), $T_2$ **nosel** $y_2$, $T_3$ **nosel** $y_2$.
- If $T_1 = \{B(r) : T_4..T_5\}$, then by induction, there exist $T_6$, $T_7$, $T_8$, $T_9$, such that $T_4 \longmapsto^{\mathrm{e}}_{\ominus} T_6$, and $T_5 \longmapsto^{\mathrm{e}}_{\oplus} T_7$, and $T_4 \longmapsto^{\mathrm{e}}_{\oplus} T_8$, and $T_5 \longmapsto^{\mathrm{e}}_{\ominus} T_9$, and $T_6$ **nosel** $y_2$, and $T_7$ **nosel** $y_2$, and $T_8$ **nosel** $y_2$, and $T_9$ **nosel** $y_2$, then choose $T_2 = \{B(r) : T_6..T_7\}$, and $T_3 = \{B(r) : T_8..T_9\}$. By (TR$^{\mathrm{m}}$-Typ), $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$. By (TN-Typ), $T_2$ **nosel** $y_2$, $T_3$ **nosel** $y_2$.
- If $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, then choose $T_2 = \top$, and $T_3 = \bot$. By (TR$^{\mathrm{m}}$-MetU), $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$. By (TR$^{\mathrm{m}}$-MetL), $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$. By (TN-Top), $T_2$ **nosel** $y_2$. By (TN-Bot), $T_3$ **nosel** $y_2$.

□

**Lemma 5.104** (TRedU). *If $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_2$, and $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_3$, then $T_2 = T_3$.*

*Idea.* $\longmapsto^{\mathrm{m}}$ is deterministic ▽

*Proof.* Induction on $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_2$:

- Case (TR$^{\mathrm{m}}$-Top): $T_1 = \top$, and $T_2 = \top$. By inversion of (TR$^{\mathrm{m}}$-Top), $T_3 = \top$.
- Case (TR$^{\mathrm{m}}$-Bot): $T_1 = \bot$, and $T_2 = \bot$. By inversion of (TR$^{\mathrm{m}}$-Bot), $T_3 = \bot$.
- Case (TR$^{\mathrm{m}}$-N): $T_1 = \mathsf{N}$, and $T_2 = \mathsf{N}$, and $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-N), $T_3 = \mathsf{N}$.
- Case (TR$^{\mathrm{m}}$-N-Bot): $T_1 = \mathsf{N}$, and $T_2 = \bot$, and $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-N-Bot), $T_3 = \bot$.
- Case (TR$^{\mathrm{m}}$-Sel): $T_1 = x_1.B(x_2)$, and $T_2 = x_1.B(x_2)$. By inversion of (TR$^{\mathrm{m}}$-Sel), $T_3 = x_1.B(x_2)$.
- Case (TR$^{\mathrm{m}}$-Rec): $T_1 = \mu(s : T)$, and $T_2 = \mu(s : T)$. By inversion of (TR$^{\mathrm{m}}$-Rec), $T_3 = \mu(s : T)$.
- Case (TR$^{\mathrm{m}}$-And): $T_1 = T_4 \wedge T_5$, and $T_2 = T_6 \wedge T_7$, where $T_4 \longmapsto^{\mathrm{m}}_{\delta} T_6$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_7$. By inversion of (TR$^{\mathrm{m}}$-And), $T_3 = T_8 \wedge T_9$, where $T_4 \longmapsto^{\mathrm{m}}_{\delta} T_8$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_9$. By induction, $T_8 = T_6$, and $T_9 = T_7$.
- Case (TR$^{\mathrm{m}}$-Or): $T_1 = T_4 \vee T_5$, and $T_2 = T_6 \vee T_7$, where $T_4 \longmapsto^{\mathrm{m}}_{\delta} T_6$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_7$. By inversion of (TR$^{\mathrm{m}}$-Or), $T_3 = T_8 \vee T_9$, where $T_4 \longmapsto^{\mathrm{m}}_{\delta} T_8$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_9$. By induction, $T_8 = T_6$, and $T_9 = T_7$.
- Case (TR$^{\mathrm{m}}$-Fld): $T_1 = \{a : T_4..T_5\}$, and $T_2 = \{a : T_6..T_7\}$, where $T_4 \longmapsto^{\mathrm{m}}_{-\delta} T_6$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_7$. By inversion of (TR$^{\mathrm{m}}$-Fld), $T_3 = \{a : T_8..T_9\}$, where $T_4 \longmapsto^{\mathrm{m}}_{-\delta} T_8$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_9$. By induction, $T_8 = T_6$, and $T_9 = T_7$.

- Case (TR$^{\mathrm{m}}$-Typ): $T_1 = \{B(r) : T_4..T_5\}$, and $T_2 = \{B(r) : T_6..T_7\}$, where $T_4 \longmapsto^{\mathrm{m}}_{-\delta} T_6$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_7$. By inversion of (TR$^{\mathrm{m}}$-Typ), $T_3 = \{B(r) : T_8..T_9\}$, where $T_4 \longmapsto^{\mathrm{m}}_{-\delta} T_8$, where $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_9$. By induction, $T_8 = T_6$, and $T_9 = T_7$.
- Case (TR$^{\mathrm{m}}$-MetU): $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_2 = \top$, and $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-MetU), $T_3 = \top$.
- Case (TR$^{\mathrm{m}}$-MetL): $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_2 = \bot$, and $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-MetL), $T_3 = \bot$.

□

**Lemma 5.105** (ERedCom). *If $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_3$, and $T_2$ **nosel** $x$, and $T_3$ **nosel** $x$, then there exists $T_4$, such that $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_4$, and $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$, and $T_4$ **nosel** $x$. If $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_3$, and $T_2$ **nosel** $x$, and $T_3$ **nosel** $x$, then there exists $T_4$, such that $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_4$, and $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$, and $T_4$ **nosel** $x$.*

*Proof.* Induction on $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_2$:

- Case (TER-Top): $T_1 = \top$, and $T_2 = \top$. By inversion of (TER-Top), $T_3 = \top$. Choose $T_4 = \top$. By (TER-Top), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-Top), $T_4$ **nosel** $x$.
- Case (TER-Bot): $T_1 = \bot$, and $T_2 = \bot$. By inversion of (TER-Bot), $T_3 = \bot$. Choose $T_4 = \bot$. By (TER-Bot), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-Bot), $T_4$ **nosel** $x$.
- Case (TER-N): $T_1 = \mathsf{N}$, and $T_2 = \mathsf{N}$, and $\delta = \oplus$. By inversion of (TER-N), $T_3 = \mathsf{N}$. Choose $T_4 = \mathsf{N}$. By (TER-N), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (TN-N), $T_4$ **nosel** $x$.
- Case (TER-N-Bot): $T_1 = \mathsf{N}$, and $T_2 = \bot$, and $\delta = \ominus$. By inversion of (TER-N-Bot), $T_3 = \bot$. Choose $T_4 = \bot$. By (TER-N-Bot), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (TN-Bot), $T_4$ **nosel** $x$.
- Case (TER-And): $T_1 = T_5 \wedge T_6$, and $T_2 = T_7 \wedge T_8$, such that $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_7$, such that $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_8$. By inversion of (TER-And). $T_3 = T_9 \wedge T_{10}$, where $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By inversion of (TN-And), $T_7$ **nosel** $x$, and $T_8$ **nosel** $x$, and $T_9$ **nosel** $x$, and $T_{10}$ **nosel** $x$.
  - If $\delta = \oplus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $\Gamma;\rho \vdash T_7 <: T_{11}$, and $\Gamma;\rho \vdash T_9 <: T_{11}$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_8 <: T_{12}$, and $\Gamma;\rho \vdash T_{10} <: T_{12}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = T_{11} \wedge T_{12}$. By (TER-And), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By 5.18(AndSub), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (TN-And), $T_4$ **nosel** $x$.
  - Otherwise, $\delta = \ominus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $\Gamma;\rho \vdash T_{11} <: T_7$, and $\Gamma;\rho \vdash T_{11} <: T_9$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_{12} <: T_8$, and $\Gamma;\rho \vdash T_{12} <: T_{10}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = T_{11} \wedge T_{12}$. By (TER-And), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By 5.18(AndSub), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-And), $T_4$ **nosel** $x$.
- Case (TER-Or): $T_1 = T_5 \vee T_6$, and $T_2 = T_7 \vee T_8$, such that $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_7$, such that $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_8$. By inversion of (TER-Or). $T_3 = T_9 \vee T_{10}$, where $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By inversion of (TN-Or), $T_7$ **nosel** $x$, and $T_8$ **nosel** $x$, and $T_9$ **nosel** $x$, and $T_{10}$ **nosel** $x$.
  - If $\delta = \oplus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $\Gamma;\rho \vdash T_7 <: T_{11}$, and $\Gamma;\rho \vdash T_9 <: T_{11}$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_8 <: T_{12}$, and $\Gamma;\rho \vdash T_{10} <: T_{12}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = T_{11} \vee T_{12}$. By (TER-Or), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By 5.19(OrSub), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (TN-Or), $T_4$ **nosel** $x$.
  - Otherwise, $\delta = \ominus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $\Gamma;\rho \vdash T_{11} <: T_7$, and $\Gamma;\rho \vdash T_{11} <: T_9$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_{12} <: T_8$, and $\Gamma;\rho \vdash T_{12} <: T_{10}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = T_{11} \vee T_{12}$. By (TER-Or), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By 5.19(OrSub), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-Or), $T_4$ **nosel** $x$.
- Case (TER-Sel): $T_1 = x_1.B(x_2)$, and $T_2 = x_1.B(x_2)$. Choose $T_4 = T_1$. By (TER-Sel), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. Trivially, $T_4$ **nosel** $x$. By inversion:
  - Case (TER-Sel): $T_3 = x_1.B(x_2)$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$.

  - Case (TER-SelL): $T_3 = \top$, and $\delta = \ominus$. By (ST-Top), $\Gamma;\rho \vdash T_4 <: T_3$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$.
  - Case (TER-SelU): $T_3 = \bot$, and $\delta = \oplus$. By (ST-Bot), $\Gamma;\rho \vdash T_3 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$.

- Case (TER-SelL): $T_1 = x_1.B(x_2)$, and $T_2 = \top$, and $\delta = \ominus$. By inversion:

  - Case (TER-Sel): $T_3 = x_1.B(x_2)$. Choose $T_4 = T_1$. Trivially, $T_4$ **nosel** $x$. By (TER-Sel), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Top), $\Gamma;\rho \vdash T_4 <: T_2$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_3$.
  - Case (TER-SelL): $T_3 = \top$. Choose $T_4 = \top$. By (TN-Top), $T_4$ **nosel** $x$. By (TER-SelL), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_3$.

- Case (TER-SelU): $T_1 = x_1.B(x_2)$, and $T_2 = \bot$, and $\delta = \oplus$. By inversion:

  - Case (TER-Sel): $T_3 = x_1.B(x_2)$. Choose $T_4 = T_1$. Trivially, $T_4$ **nosel** $x$. By (TER-Sel), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Bot), $\Gamma;\rho \vdash T_2 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_3 <: T_4$.
  - Case (TER-SelU): $T_3 = \bot$. Choose $T_4 = \bot$. By (TN-Bot), $T_4$ **nosel** $x$. By (TER-SelU), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_3 <: T_4$.

- Case (TER-Rec): $T_1 = \mu(s : T_7)$, and $T_2 = \mu(s : T_7)$. By inversion of (TER-Rec), $T_3 = \mu(s : T_7)$. Choose $T_4 = \mu(s : T_7)$. By (TER-Rec), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. Trivially, $T_4$ **nosel** $x$.
- Case (TER-Fld): $T_1 = \{a : T_5..T_6\}$, and $T_2 = \{a : T_7..T_8\}$, such that $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_7$, such that $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_8$. By inversion of (TER-Fld). $T_3 = \{a : T_9..T_{10}\}$, where $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By inversion of (TN-Fld), $T_7$ **nosel** $x$, and $T_8$ **nosel** $x$, and $T_9$ **nosel** $x$, and $T_{10}$ **nosel** $x$.

  - If $\delta = \oplus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, and $\Gamma;\rho \vdash T_{11} <: T_7$, and $\Gamma;\rho \vdash T_{11} <: T_9$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_8 <: T_{12}$, and $\Gamma;\rho \vdash T_{10} <: T_{12}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = \{a : T_{11}..T_{12}\}$. By (TER-Fld), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Fld), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (TN-Fld), $T_4$ **nosel** $x$.
  - Otherwise, $\delta = \ominus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, and $\Gamma;\rho \vdash T_7 <: T_{11}$, and $\Gamma;\rho \vdash T_9 <: T_{11}$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_{12} <: T_8$, and $\Gamma;\rho \vdash T_{12} <: T_{10}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = \{a : T_{11}..T_{12}\}$. By (TER-Fld), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Fld), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-Fld), $T_4$ **nosel** $x$.

- Case (TER-Typ): $T_1 = \{B(r) : T_5..T_6\}$, and $T_2 = \{B(r) : T_7..T_8\}$, such that $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_7$, such that $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_8$. By inversion of (TER-Typ). $T_3 = \{B(r) : T_9..T_{10}\}$, where $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By inversion of (TN-Typ), $T_7$ **nosel** $x$, and $T_8$ **nosel** $x$, and $T_9$ **nosel** $x$, and $T_{10}$ **nosel** $x$.

  - If $\delta = \oplus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, and $\Gamma;\rho \vdash T_{11} <: T_7$, and $\Gamma;\rho \vdash T_{11} <: T_9$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_8 <: T_{12}$, and $\Gamma;\rho \vdash T_{10} <: T_{12}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = \{B(r) : T_{11}..T_{12}\}$. By (TER-Typ), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Typ), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (TN-Typ), $T_4$ **nosel** $x$.
  - Otherwise, $\delta = \ominus$. By induction, exist $T_{11}$, $T_{12}$, such that $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, and $\Gamma;\rho \vdash T_7 <: T_{11}$, and $\Gamma;\rho \vdash T_9 <: T_{11}$, and $T_{11}$ **nosel** $x$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\Gamma;\rho \vdash T_{12} <: T_8$, and $\Gamma;\rho \vdash T_{12} <: T_{10}$, and $T_{12}$ **nosel** $x$. Choose $T_4 = \{B(r) : T_{11}..T_{12}\}$. By (TER-Typ), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Typ), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-Typ), $T_4$ **nosel** $x$.

- Case (TER-MetU): $T_1 = \{m(z : T_5, r : T_7) : T_6\}$, and $T_2 = \top$, and $\delta = \oplus$. By inversion of (TER-MetU). $T_3 = \top$. Choose $T_4 = \top$. By (TER-MetU), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-Top), $T_4$ **nosel** $x$.
- Case (TER-MetL): $T_1 = \{m(z : T_5, r : T_7) : T_6\}$, and $T_2 = \bot$, and $\delta = \ominus$. By inversion of (TER-MetL). $T_3 = \bot$. Choose $T_4 = \bot$. By (TER-MetL), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_2 <: T_4$, and $\Gamma;\rho \vdash T_3 <: T_4$. By (ST-Refl), $\Gamma;\rho \vdash T_4 <: T_2$, and $\Gamma;\rho \vdash T_4 <: T_3$. By (TN-Bot), $T_4$ **nosel** $x$.

□

**Lemma 5.106** (TRedEq). *If $\rho \vdash T_1 \approx T_2$, and $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_3$, then there exists $T_4$, such that $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4$, and $\rho \vdash T_3 \approx T_4$.*

*Idea.* M reduction preserves equivalence ▽

*Proof.* Induction on $\rho \vdash T_1 \approx T_2$:

- Case (TE-Refl): $T_1 = T_2$. Choose $T_4 = T_3$. By (TE-Refl).
- Case (TE-Sel): $T_1 = v_1.A(x_2)$, and $T_2 = v_2.A(x_2)$, where $\rho \vdash v_1 \approx v_2$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Sel), $T_3 = T_1$. Choose $T_4 = T_2$. By ($\mathrm{TR}^{\mathrm{m}}$-Sel).
- Case (TE-And): $T_1 = T_5 \wedge T_6$, and $T_2 = T_7 \wedge T_8$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-And), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \wedge T_{10}$, and $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_9$, and $T_6 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $T_9 \longmapsto^{\mathrm{m}}_{\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \wedge T_{12}$. By (TE-And) and ($\mathrm{TR}^{\mathrm{m}}$-And).
- Case (TE-Or): $T_1 = T_5 \vee T_6$, and $T_2 = T_7 \vee T_8$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Or), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \vee T_{10}$, and $T_5 \longmapsto^{\mathrm{m}}_{\delta} T_9$, and $T_6 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $T_9 \longmapsto^{\mathrm{m}}_{\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \vee T_{12}$. By (TE-Or) and ($\mathrm{TR}^{\mathrm{m}}$-Or).
- Case (TE-Rec): $T_1 = \mu(s : T_5)$, and $T_2 = \mu(s : T_7)$, and $\rho \vdash T_5 \approx T_7$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Rec), $T_3 = T_1$. Choose $T_4 = T_2$. By ($\mathrm{TR}^{\mathrm{m}}$-Rec).
- Case (TE-Typ): $T_1 = \{B(r) : T_5..T_6\}$, and $T_2 = \{B(r) : T_7..T_8\}$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Typ), exist $T_9$, $T_{10}$, such that $T_3 = \{B(r) : T_9..T_{10}\}$, and $T_5 \longmapsto^{\mathrm{m}}_{-\delta} T_9$, and $T_6 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $T_9 \longmapsto^{\mathrm{m}}_{-\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = \{B(r) : T_{11}..T_{12}\}$. By (TE-Typ) and ($\mathrm{TR}^{\mathrm{m}}$-Typ).
- Case (TE-Fld): $T_1 = \{a : T_5..T_6\}$, and $T_2 = \{a : T_7..T_8\}$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Fld), exist $T_9$, $T_{10}$, such that $T_3 = \{a : T_9..T_{10}\}$, and $T_5 \longmapsto^{\mathrm{m}}_{-\delta} T_9$, and $T_6 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $T_9 \longmapsto^{\mathrm{m}}_{-\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = \{a : T_{11}..T_{12}\}$. By (TE-Fld) and ($\mathrm{TR}^{\mathrm{m}}$-Fld).
- Case (TE-Met): $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, and $T_2 = \{m(z : T_{10}, r : T_{12}) : T_{11}\}$. If $\delta = \oplus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-MetU), $T_3 = \top$. Choose $T_4 = \top$. By ($\mathrm{TR}^{\mathrm{m}}$-MetU) and (TE-Refl). Otherwise, $\delta = \ominus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-MetL), $T_3 = \bot$. Choose $T_4 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-MetL) and (TE-Refl).

□

**Lemma 5.107** (TRedCom). *If* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\oplus} T_1 <: T_2$*, and* $T_1 \longmapsto^{\mathrm{m}}_{\oplus} T_3$*, then there exists* $T_4$*, such that* $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$*, and* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$*. If* $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\ominus} T_1 <: T_2$*, and* $T_2 \longmapsto^{\mathrm{m}}_{\ominus} T_6$*, then there exists* $T_5$*, such that* $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$*, and* $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$*.*

*Idea.* If we have subtyping of $T_1$ and $T_2$, which uses selection subtyping only in one direction, in an inert context, and if we reduce the type on one side by replacing method types by $\top$ or $\bot$ in the same direction, then we can reduce the other type so that we have subtyping between the reduced types, which does not use method subtyping. (Occurrences in recursive types are overlooked.) ▽

*Proof.* Induction on $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_2$:

- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Top): $T_2 = \top$. Choose $T_4 = \top$. By ($\mathrm{TR}^{\mathrm{m}}$-Top), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Top), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Top), $T_6 = \top$. By 5.102(TRedEx), exists $T_5$, such that $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Top), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.
- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Bot): $T_1 = \bot$. Choose $T_5 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Bot), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Bot), $T_3 = \bot$. By 5.102(TRedEx), exists $T_4$, such that $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Bot), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Refl): $T_1 = T_2$. Choose $T_4 = T_3$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Refl), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$. Choose $T_5 = T_6$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Refl), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.
- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-Rec): $T_1 = \mathsf{N}$, and $T_2 = \mu(s : T_7)$.
  - If $\delta = \oplus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-N), $T_3 = \mathsf{N}$. Choose $T_4 = T_2$. By ($\mathrm{TR}^{\mathrm{m}}$-Rec), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-N-Rec), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-Rec), $T_6 = \mu(s : T_7)$. Choose $T_5 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-N-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Bot), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.
- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-M): $T_1 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_2 = \bot$.

- If $\delta = \oplus$, then by inversion of (TR$^{\mathrm{m}}$-And), and by inversion of (TR$^{\mathrm{m}}$-N) and 5.100(TRedMut), $T_3 = T_1$. Choose $T_4 = T_2$. By (TR$^{\mathrm{m}}$-Bot), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By (ST$^{\mathrm{m}}_{\#}$-N-M), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
- Otherwise, $\delta = \ominus$, then by inversion of (TR$^{\mathrm{m}}$-Bot), $T_6 = T_2$. Choose $T_5 = \bot \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By (TR$^{\mathrm{m}}$-Bot) and (TR$^{\mathrm{m}}$-Typ) and (TR$^{\mathrm{m}}$-N-Bot) and (TR$^{\mathrm{m}}$-And), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST$^{\mathrm{m}}_{\#}$-N-M), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: T_6$. By (ST$^{\mathrm{m}}_{\#}$-Bot) and (ST$^{\mathrm{m}}_{\#}$-Refl) and 5.90(AndSubM), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By (ST$^{\mathrm{m}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-And1): $T_1 = T_2 \wedge T_7$.
  - If $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-And), $T_3 = T_8 \wedge T_9$, such that $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$. Choose $T_4 = T_8$. By (ST$^{\mathrm{m}}_{\#}$-And1), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By 5.102(TRedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_8$. Choose $T_5 = T_6 \wedge T_8$. By (TR$^{\mathrm{m}}$-And), $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_5$. By (ST$^{\mathrm{m}}_{\#}$-And1), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-And2): $T_1 = T_7 \wedge T_2$.
  - If $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-And), $T_3 = T_9 \wedge T_8$, such that $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$. Choose $T_4 = T_8$. By (ST$^{\mathrm{m}}_{\#}$-And2), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By 5.102(TRedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_8$. Choose $T_5 = T_8 \wedge T_6$. By (TR$^{\mathrm{m}}$-And), $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_5$. By (ST$^{\mathrm{m}}_{\#}$-And2), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-And): $T_2 = T_7 \wedge T_8$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_8$.
  - If $\delta = \oplus$. By induction, exists $T_9$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_9$. By induction, exists $T_{10}$, such that $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_{10}$. Choose $T_4 = T_9 \wedge T_{10}$. By (TR$^{\mathrm{m}}$-And), $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4$. By (ST$^{\mathrm{m}}_{\#}$-And), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-And), exist $T_9$, $T_{10}$, such that $T_6 = T_9 \wedge T_{10}$, and $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$, and $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$. By induction, exist $T_5$, $T_{11}$, such that $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_9$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_{11} <: T_{10}$, and $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_5$, and $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_{11}$. By 5.104(TRedU), $T_{11} = T_5$. By (ST$^{\mathrm{m}}_{\#}$-And), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-Or1): $T_2 = T_1 \vee T_7$.
  - If $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-Or), $T_6 = T_8 \vee T_9$, such that $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$. Choose $T_5 = T_8$. By (ST$^{\mathrm{m}}_{\#}$-Or1), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_6$.
  - Otherwise, $\delta = \oplus$. By 5.102(TRedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_8$. Choose $T_4 = T_3 \vee T_8$. By (TR$^{\mathrm{m}}$-Or), $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4$. By (ST$^{\mathrm{m}}_{\#}$-Or1), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_4$.

- Case (ST$^{\mathrm{s}}_{\#}$-Or2): $T_2 = T_7 \vee T_1$.
  - If $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-Or), $T_6 = T_9 \vee T_8$, such that $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$. Choose $T_5 = T_8$. By (ST$^{\mathrm{m}}_{\#}$-Or2), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_6$.
  - Otherwise, $\delta = \oplus$. By 5.102(TRedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_8$. Choose $T_4 = T_8 \vee T_3$. By (TR$^{\mathrm{m}}$-Or), $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4$. By (ST$^{\mathrm{m}}_{\#}$-Or2), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_4$.

- Case (ST$^{\mathrm{s}}_{\#}$-Or): $T_1 = T_7 \vee T_8$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_7 <: T_2$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_8 <: T_2$.
  - If $\delta = \ominus$. By induction, exists $T_9$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_9 <: T_6$. By induction, exists $T_{10}$, such that $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_{10} <: T_6$. Choose $T_5 = T_9 \wedge T_{10}$. By (TR$^{\mathrm{m}}$-Or), $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_5$. By (ST$^{\mathrm{m}}_{\#}$-Or), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_6$.
  - Otherwise, $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-Or), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \vee T_{10}$, and $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_9$, and $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$. By induction, exist $T_4$, $T_{11}$, such that $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_9 <: T_4$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_{10} <: T_{11}$, and $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4$, and $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_{11}$. By 5.104(TRedU), $T_{11} = T_4$. By (ST$^{\mathrm{m}}_{\#}$-Or), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_4$.

- Case (ST$^{\mathrm{s}}_{\#}$-Trans): $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_1 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_7 <: T_2$.
  - If $\delta = \oplus$. By induction, exists $T_8$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_8$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_8$. By induction, exists $T_4$, such that $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_8 <: T_4$. By (ST$^{\mathrm{m}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_3 <: T_4$.

- Otherwise, $\delta = \ominus$. By induction, exists $T_8$, such that $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_8$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_8 <: T_6$. By induction, exists $T_5$, such that $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_5$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_8$. By (ST$^{\mathrm{m}}_{\#}$-Trans), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-SelL): $T_2 = v_1.B(x_2)$, and $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_7..T_8\}$, and $T_1 = [x_2/r]T_7$, and $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-Sel), $T_2 = T_6$. By 5.102(TRedEx), exists $T_5$, such that $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST$^{\mathrm{m}}_{\#}$-SelL), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.
- Case (ST$^{\mathrm{s}}_{\#}$-SelU): $T_1 = v_1.B(x_2)$, and $\mathrm{F} \vdash_{!} v_1 : \{B(r) : T_7..T_8\}$, and $T_2 = [x_2/r]T_8$, and $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-Sel), $T_1 = T_3$. By 5.102(TRedEx), exists $T_4$, such that $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By (ST$^{\mathrm{m}}_{\#}$-SelU), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
- Case (ST$^{\mathrm{s}}_{\#}$-Typ): $T_1 = \{B(r) : T_7..T_8\}$, and $T_2 = \{B(r) : T_9..T_{10}\}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{-\delta} T_9 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_8 <: T_{10}$.

  - If $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-Typ), $T_3 = \{B(r) : T_{11}..T_{12}\}$, where $T_7 \longmapsto^{\mathrm{m}}_{\ominus} T_{11}$, and $T_8 \longmapsto^{\mathrm{m}}_{\oplus} T_{12}$. By induction, exist $T_{13}, T_{14}$, such that $T_9 \longmapsto^{\mathrm{m}}_{\ominus} T_{13}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_{13} <: T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\oplus} T_{14}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_{12} <: T_{14}$. Choose $T_4 = \{B(r) : T_{13}..T_{14}\}$. By (TR$^{\mathrm{m}}$-Typ), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By (ST$^{\mathrm{m}}_{\#}$-Typ), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-Typ), $T_6 = \{B(r) : T_{11}..T_{12}\}$, where $T_9 \longmapsto^{\mathrm{m}}_{\oplus} T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\ominus} T_{12}$. By induction, exist $T_{13}, T_{14}$, such that $T_7 \longmapsto^{\mathrm{m}}_{\oplus} T_{13}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_{11} <: T_{13}$, and $T_8 \longmapsto^{\mathrm{m}}_{\ominus} T_{14}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_{14} <: T_{12}$. Choose $T_5 = \{B(r) : T_{13}..T_{14}\}$. By (TR$^{\mathrm{m}}$-Typ), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST$^{\mathrm{m}}_{\#}$-Typ), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-Fld): $T_1 = \{a : T_7..T_8\}$, and $T_2 = \{a : T_9..T_{10}\}$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{-\delta} T_9 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathrm{s}}_{\delta} T_8 <: T_{10}$.

  - If $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-Fld), $T_3 = \{a : T_{11}..T_{12}\}$, where $T_7 \longmapsto^{\mathrm{m}}_{\ominus} T_{11}$, and $T_8 \longmapsto^{\mathrm{m}}_{\oplus} T_{12}$. By induction, exist $T_{13}, T_{14}$, such that $T_9 \longmapsto^{\mathrm{m}}_{\ominus} T_{13}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_{13} <: T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\oplus} T_{14}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_{12} <: T_{14}$. Choose $T_4 = \{a : T_{13}..T_{14}\}$. By (TR$^{\mathrm{m}}$-Fld), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By (ST$^{\mathrm{m}}_{\#}$-Fld), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-Fld), $T_6 = \{a : T_{11}..T_{12}\}$, where $T_9 \longmapsto^{\mathrm{m}}_{\oplus} T_{11}$, and $T_{10} \longmapsto^{\mathrm{m}}_{\ominus} T_{12}$. By induction, exist $T_{13}, T_{14}$, such that $T_7 \longmapsto^{\mathrm{m}}_{\oplus} T_{13}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_{11} <: T_{13}$, and $T_8 \longmapsto^{\mathrm{m}}_{\ominus} T_{14}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_{14} <: T_{12}$. Choose $T_5 = \{a : T_{13}..T_{14}\}$. By (TR$^{\mathrm{m}}$-Fld), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST$^{\mathrm{m}}_{\#}$-Fld), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-Met): $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, and $T_2 = \{m(z : T_{10}, r : T_{12}) : T_{11}\}$.

  - If $\delta = \oplus$. By inversion of (TR$^{\mathrm{m}}$-MetU), $T_3 = \top$. Choose $T_4 = \top$. By (TR$^{\mathrm{m}}$-MetU), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By (ST$^{\mathrm{m}}_{\#}$-Refl), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By inversion of (TR$^{\mathrm{m}}$-MetL), $T_6 = \bot$. Choose $T_5 = \bot$. By (TR$^{\mathrm{m}}$-MetL), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST$^{\mathrm{m}}_{\#}$-Refl), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-TypAnd): $T_1 = \{B(r) : T_7..T_8\} \wedge \{B(r) : T_9..T_{10}\}$, and $T_2 = \{B(r) : T_7 \vee T_9..T_8 \wedge T_{10}\}$.

  - If $\delta = \oplus$, then by inversion of (TR$^{\mathrm{m}}$-And), and by inversion of (TR$^{\mathrm{m}}$-Typ), $T_3 = \{B(r) : T_{11}..T_{12}\} \wedge \{B(r) : T_{13}..T_{14}\}$, where $T_7 \longmapsto^{\mathrm{m}}_{-\delta} T_{11}$, where $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{12}$, where $T_9 \longmapsto^{\mathrm{m}}_{-\delta} T_{13}$, where $T_{10} \longmapsto^{\mathrm{m}}_{\delta} T_{14}$. Choose $T_4 = \{B(r) : T_{11} \vee T_{13}..T_{12} \wedge T_{14}\}$. By (TR$^{\mathrm{m}}$-Typ) and (TR$^{\mathrm{m}}$-And), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By (ST$^{\mathrm{m}}_{\#}$-TypAnd), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of (TR$^{\mathrm{m}}$-Typ), and by inversion of (TR$^{\mathrm{m}}$-And), and by inversion of (TR$^{\mathrm{m}}$-Or), $T_6 = \{B(r) : T_{11} \vee T_{13}..T_{12} \wedge T_{14}\}$, where $T_7 \longmapsto^{\mathrm{m}}_{-\delta} T_{11}$, where $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{12}$, where $T_9 \longmapsto^{\mathrm{m}}_{-\delta} T_{13}$, where $T_{10} \longmapsto^{\mathrm{m}}_{\delta} T_{14}$. Choose $T_5 = \{B(r) : T_{11}..T_{12}\} \wedge \{B(r) : T_{13}..T_{14}\}$. By (TR$^{\mathrm{m}}$-And) and (TR$^{\mathrm{m}}$-Or) and (TR$^{\mathrm{m}}$-Typ), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST$^{\mathrm{m}}_{\#}$-TypAnd), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case (ST$^{\mathrm{s}}_{\#}$-Eq): $\rho \vdash T_1 \approx T_2$.

  - If $\delta = \oplus$. By 5.106(TRedEq), exists $T_4$, such that $\rho \vdash T_3 \approx T_4$, and $T_2 \longmapsto^{\mathrm{m}}_{\delta} T_4$. By (ST$^{\mathrm{m}}_{\#}$-Eq).
  - Otherwise, $\delta = \ominus$. By 5.2(EqSymm), $\rho \vdash T_2 \approx T_1$. By 5.106(TRedEq), exists $T_5$, such that $\rho \vdash T_6 \approx T_5$, and $T_1 \longmapsto^{\mathrm{m}}_{\delta} T_5$. By 5.2(EqSymm), $\rho \vdash T_5 \approx T_6$. By (ST$^{\mathrm{m}}_{\#}$-Eq).

- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-Fld): $T_1 = \mathsf{N}$, and $T_2 = \{a : T_7..T_8\}$.
  - If $\delta = \oplus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-N), $T_3 = \mathsf{N}$. By 5.102(TRedEx), exist $T_9$, $T_{10}$, such that $T_7 \longmapsto^{\mathrm{m}}_{\ominus} T_9$, such that $T_8 \longmapsto^{\mathrm{m}}_{\oplus} T_{10}$. Choose $T_4 = \{a : T_9..T_{10}\}$. By ($\mathrm{TR}^{\mathrm{m}}$-Fld), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-N-Fld), F;$\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-Fld), $T_6 = \{a : T_9..T_{10}\}$. Choose $T_5 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-N-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Bot), F;$\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-Met): $T_1 = \mathsf{N}$, and $T_2 = \{m(z : T_7, r : T_9) : T_8\}$.
  - If $\delta = \oplus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-N), $T_3 = \mathsf{N}$. Choose $T_4 = \top$. By ($\mathrm{TR}^{\mathrm{m}}$-MetU), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Top), F;$\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-MetL), $T_6 = \bot$. Choose $T_5 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-N-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Refl), F;$\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-N-Typ): $T_1 = \mathsf{N}$, and $T_2 = \{A(r) : T_7..T_8\}$.
  - If $\delta = \oplus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-N), $T_3 = \mathsf{N}$. By 5.102(TRedEx), exist $T_9$, $T_{10}$, such that $T_7 \longmapsto^{\mathrm{m}}_{\ominus} T_9$, such that $T_8 \longmapsto^{\mathrm{m}}_{\oplus} T_{10}$. Choose $T_4 = \{A(r) : T_9..T_{10}\}$. By ($\mathrm{TR}^{\mathrm{m}}$-Typ), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-N-Typ), F;$\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-Typ), $T_6 = \{A(r) : T_9..T_{10}\}$. Choose $T_5 = \bot$. By ($\mathrm{TR}^{\mathrm{m}}$-N-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Bot), F;$\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

- Case ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Dist): $T_1 = T_7 \wedge (T_8 \vee T_9)$. $T_2 = (T_7 \wedge T_8) \vee (T_7 \wedge T_9)$.
  - If $\delta = \oplus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-And), and by inversion of ($\mathrm{TR}^{\mathrm{m}}$-Or), $T_3 = T_{10} \wedge T_{11} \vee T_{12}$, where $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_{10}$, where $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{11}$, where $T_9 \longmapsto^{\mathrm{m}}_{\delta} T_{12}$. Choose $T_4 = (T_{10} \wedge T_{11}) \vee (T_{10} \wedge T_{12})$. By ($\mathrm{TR}^{\mathrm{m}}$-And) and ($\mathrm{TR}^{\mathrm{m}}$-Or), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Dist), F;$\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of ($\mathrm{TR}^{\mathrm{m}}$-Or), and by inversion of ($\mathrm{TR}^{\mathrm{m}}$-And), $T_6 = (T_{11} \wedge T_{13}) \vee (T_{12} \wedge T_{14})$, where $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_{11}$, where $T_7 \longmapsto^{\mathrm{m}}_{\delta} T_{12}$, where $T_8 \longmapsto^{\mathrm{m}}_{\delta} T_{13}$, where $T_9 \longmapsto^{\mathrm{m}}_{\delta} T_{14}$. By 5.104(TRedU), $T_{11} = T_{12}$. Choose $T_5 = T_{11} \wedge (T_{13} \vee T_{14})$. By ($\mathrm{TR}^{\mathrm{m}}$-And) and ($\mathrm{TR}^{\mathrm{m}}$-Or), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Dist), F;$\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$.

□

**Lemma 5.108** (ToTRed). *If* F;$\rho \vdash^{\mathrm{s}}_{\oplus} T_1 <: T_2$*, then there exist* $T_3$*,* $T_4$*, such that* $T_1 \longmapsto^{\mathrm{m}}_{\oplus} T_3$*, and* $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$*, and* F;$\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$.

*Proof.* By 5.102(TRedEx), exists $T_3$, such that $T_1 \longmapsto^{\mathrm{m}}_{\oplus} T_3$. By 5.107(TRedCom), exists $T_4$, such that $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$, and F;$\rho \vdash^{\mathrm{m}}_{\oplus} T_3 <: T_4$. □

**Lemma 5.109** (ERedEq). *If* $\rho \vdash T_1 \approx T_2$*, and* $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_3$*, then there exists* $T_4$*, such that* $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$*, and* $\rho \vdash T_3 \approx T_4$.

*Idea.* E reduction preserves equivalence ▽

*Proof.* Induction on $\rho \vdash T_1 \approx T_2$:

- Case (TE-Refl): $T_1 = T_2$. Choose $T_4 = T_3$. By (TE-Refl).
- Case (TE-Sel): $T_1 = v_1.A(x_2)$, and $T_2 = v_2.A(x_2)$, where $\rho \vdash v_1 \approx v_2$. By inversion:
  - Case (TER-Sel): $T_3 = T_1$. Choose $T_4 = T_2$. By (TER-Sel).
  - Case (TER-SelU): $T_3 = \bot$. Choose $T_4 = \bot$. By (TER-SelU) and (TE-Refl).
  - Case (TER-SelL): $T_3 = \top$. Choose $T_4 = \top$. By (TER-SelU) and (TE-Refl).
- Case (TE-And): $T_1 = T_5 \wedge T_6$, and $T_2 = T_7 \wedge T_8$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of (TER-And), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \wedge T_{10}$, and $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $T_9 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \wedge T_{12}$. By (TE-And) and (TER-And).

- Case (TE-Or): $T_1 = T_5 \vee T_6$, and $T_2 = T_7 \vee T_8$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of (TER-Or), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \vee T_{10}$, and $T_5 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By induction, exist $T_{11}, T_{12}$, such that $T_9 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = T_{11} \vee T_{12}$. By (TE-Or) and (TER-Or).
- Case (TE-Rec): $T_1 = \mu(s : T_5)$, and $T_2 = \mu(s : T_7)$, and $\rho \vdash T_5 \approx T_7$. By inversion of (TER-Rec), $T_3 = T_1$. Choose $T_4 = T_2$. By (TER-Rec).
- Case (TE-Typ): $T_1 = \{B(r) : T_5..T_6\}$, and $T_2 = \{B(r) : T_7..T_8\}$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of (TER-Typ), exist $T_9$, $T_{10}$, such that $T_3 = \{B(r) : T_9..T_{10}\}$, and $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $T_9 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = \{B(r) : T_{11}..T_{12}\}$. By (TE-Typ) and (TER-Typ).
- Case (TE-Fld): $T_1 = \{a : T_5..T_6\}$, and $T_2 = \{a : T_7..T_8\}$, and $\rho \vdash T_5 \approx T_7$, and $\rho \vdash T_6 \approx T_8$. By inversion of (TER-Fld), exist $T_9$, $T_{10}$, such that $T_3 = \{a : T_9..T_{10}\}$, and $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_9$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By induction, exist $T_{11}$, $T_{12}$, such that $T_9 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $\rho \vdash T_7 \approx T_{11}$, and $\rho \vdash T_8 \approx T_{12}$. Choose $T_4 = \{a : T_{11}..T_{12}\}$. By (TE-Fld) and (TER-Fld).
- Case (TE-Met): $T_1 = \{m(z : T_7, r : T_9) : T_8\}$, and $T_2 = \{m(z : T_{10}, r : T_{12}) : T_{11}\}$. If $\delta = \oplus$, then by inversion of (TER-MetU), $T_3 = \top$. Choose $T_4 = \top$. By (TER-MetU) and (TE-Refl). Otherwise, $\delta = \ominus$, then by inversion of (TER-MetL), $T_3 = \bot$. Choose $T_4 = \bot$. By (TER-MetL) and (TE-Refl).

□

### 5.2.8 Context shortening lemmata

This section states properties about typing relations that can be derived in a shorter context. They are required for proving preservation of the **mreach** relation.

**Lemma 5.110** (PrecCut). *If* $\mathrm{F} = \mathrm{F}_1, v : T_1, \mathrm{F}_2$*, and* $\mathrm{F} \vdash_! v : T_2$*, then* $\mathrm{F}_1, v : T_1 \vdash_! v : T_2$.

*Idea.* Precise typing of a variable is not affected by later variables. ▽

*Proof idea.* Straightforward induction on precise typing. ▽

*Proof.* Induction on precise typing:

- Case (VT$_!$-Var): By (VT$_!$-Var), with $\mathrm{F}_1, v : T_1$.
- Case (VT$_!$-Rec): By induction and (VT$_!$-Rec).
- Case (VT$_!$-And1): By induction and (VT$_!$-And1).
- Case (VT$_!$-And2): By induction and (VT$_!$-And2).

□

**Lemma 5.111** (PrecFV). *If* $\mathrm{F} = \mathrm{F}_1, v : T_1, \mathrm{F}_2$*, and* $\mathrm{F} \vdash_! v : T_2$*, then* $\mathrm{fv}\ T_2 \cap \mathrm{dom}\ \mathrm{F}_2 = \emptyset$.

*Idea.* Precise type of a variable only contains variables from the context. ▽

*Proof idea.* Straightforward induction on precise typing. ▽

*Proof.* Induction on precise typing:

- Case (VT$_!$-Var): By inertness of F.
- Case (VT$_!$-Rec): By induction. By $v \notin \mathrm{dom}\ \mathrm{F}_2$ and (VT$_!$-Rec).
- Case (VT$_!$-And1): By induction and (VT$_!$-And1).
- Case (VT$_!$-And2): By induction and (VT$_!$-And2).

□

**Lemma 5.112** (NoselFV). *If* $v \notin \mathrm{fv}\ T_1$*, then* $T_1$ **nosel** $v$.

*Idea.* Non-occurring variables are nosel. ▽

*Proof idea.* Straightforward induction on type syntax. ▽

*Proof.*
- If $T_1 = \top$. Directly by (TN-Top).
- If $T_1 = \bot$. Directly by (TN-Bot).
- If $T_1 = \mathsf{N}$. Directly by (TN-N).
- If $T_1 = \mu(s : T_4)$. Directly by (TN-Rec).
- If $T_1 = x_1.B(x_2)$. Because $v \notin \mathrm{fv}\ T_1$, $x_1 \neq v$, and $x_2 \neq v$. By (TN-Sel).
- If $T_1 = T_4 \wedge T_5$. By induction, $T_4$ **nosel** $v$, and $T_5$ **nosel** $v$. By (TN-And).
- If $T_1 = T_4 \vee T_5$. By induction, $T_4$ **nosel** $v$, and $T_5$ **nosel** $v$. By (TN-Or).
- If $T_1 = \{a : T_4..T_5\}$. By induction, $T_4$ **nosel** $v$, and $T_5$ **nosel** $v$. By (TN-Fld).
- If $T_1 = \{B(r) : T_4..T_5\}$. By induction, $T_4$ **nosel** $v$, and $T_5$ **nosel** $v$. By (TN-Typ).
- If $T_1 = \{m(z : T_4, r : T_6) : T_5\}$. By induction, $T_4$ **nosel** $v$, and $T_5$ **nosel** $v$, and $T_6$ **nosel** $v$. By (TN-Met).

□

**Lemma 5.113** (NoselSub). *If* $T_1$ **nosel** $v$*, and* $x \neq v$*, then* $[x/r]T_1$ **nosel** $v$.

*Idea.* Substitution preserves nosel. ▽

*Proof idea.* Straightforward induction on type syntax. ▽

*Proof.* Induction on $T_1$ **nosel** $v$:

- Case (TN-Top): Directly by (TN-Top).
- Case (TN-Bot): Directly by (TN-Bot).
- Case (TN-N): Directly by (TN-N).
- Case (TN-And): $T_1 = T_2 \wedge T_3$, where $T_2$ **nosel** $v$, where $T_3$ **nosel** $v$. By induction, $[x/r]T_2$ **nosel** $v$, $[x/r]T_3$ **nosel** $v$. By (TX-And) and (TN-And).
- Case (TN-Or): $T_1 = T_2 \vee T_3$, where $T_2$ **nosel** $v$, where $T_3$ **nosel** $v$. By induction, $[x/r]T_2$ **nosel** $v$, $[x/r]T_3$ **nosel** $v$. By (TX-Or) and (TN-Or).
- Case (TN-Sel): $T_1 = x_1.B(x_2)$, where $x_1 \neq v$, and $x_2 \neq v$. By (VX-VarN), $[x/r]x_1 \neq v$, and $[x/r]x_2 \neq v$. By (TX-Sel) and (TN-Sel).
- Case (TN-Rec): Directly by (TN-Rec).
- Case (TN-Typ): $T_1 = \{B(r_2) : T_2..T_3\}$, where $T_2$ **nosel** $v$, where $T_3$ **nosel** $v$. By induction, $[x/r]T_2$ **nosel** $v$, $[x/r]T_3$ **nosel** $v$. By (TX-Typ) and (TN-Typ).
- Case (TN-Fld): $T_1 = \{a : T_2..T_3\}$, where $T_2$ **nosel** $v$, where $T_3$ **nosel** $v$. By induction, $[x/r]T_2$ **nosel** $v$, $[x/r]T_3$ **nosel** $v$. By (TX-Fld) and (TN-Fld).
- Case (TN-Met): $T_1 = \{m(z : T_2, r : T_4) : T_3\}$, where $T_2$ **nosel** $v$, where $T_3$ **nosel** $v$, where $T_4$ **nosel** $v$. By induction, $[x/r]T_2$ **nosel** $v$, $[x/r]T_3$ **nosel** $v$, $[x/r]T_4$ **nosel** $v$. By (TX-Met) and (TN-Met).

□

**Lemma 5.114** (TRedCut). *If $T_1$ **nosel** $y_2$, and $T_1 \longmapsto_{\oplus}^{\mathrm{m}} T_2$, then $\mathrm{F}_1;\rho \vdash T_1 <: T_2$, and $T_2$ **nosel** $y_2$, and $T_2 \longmapsto_{\oplus}^{\mathrm{e}} T_2$. If $T_1$ **nosel** $y_2$, and $T_1 \longmapsto_{\ominus}^{\mathrm{m}} T_2$, then $\mathrm{F}_1;\rho \vdash T_2 <: T_1$, and $T_2$ **nosel** $y_2$, and $T_2 \longmapsto_{\ominus}^{\mathrm{e}} T_2$.*

*Proof.* Induction on $T_1 \longmapsto_{\delta}^{\mathrm{m}} T_2$:

- Case (TR$^{\mathrm{m}}$-Top): $T_1 = T_2 = \top$. By (ST-Refl), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$, and $\mathrm{F}_1;\rho \vdash T_2 <: T_1$. By (TER-Top), $T_2 \longmapsto_{\delta}^{\mathrm{e}} T_2$.
- Case (TR$^{\mathrm{m}}$-Bot): $T_1 = T_2 = \bot$. By (ST-Refl), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$, and $\mathrm{F}_1;\rho \vdash T_2 <: T_1$. By (TER-Bot), $T_2 \longmapsto_{\delta}^{\mathrm{e}} T_2$.
- Case (TR$^{\mathrm{m}}$-N): $T_1 = T_2 = \mathsf{N}$, and $\delta = \oplus$. By (ST-Refl), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$. By (TER-N), $T_2 \longmapsto_{\delta}^{\mathrm{e}} T_2$.
- Case (TR$^{\mathrm{m}}$-Sel): $T_1 = T_2 = x_1.B(x_2)$. By (ST-Refl), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$, and $\mathrm{F}_1;\rho \vdash T_2 <: T_1$. By (TER-Sel), $T_2 \longmapsto_{\delta}^{\mathrm{e}} T_2$.
- Case (TR$^{\mathrm{m}}$-Rec): $T_1 = T_2 = \mu(s : T_3)$. By (ST-Refl), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$, and $\mathrm{F}_1;\rho \vdash T_2 <: T_1$. By (TER-Rec), $T_2 \longmapsto_{\delta}^{\mathrm{e}} T_2$.
- Case (TR$^{\mathrm{m}}$-N-Bot): $T_1 = \mathsf{N}$, and $T_2 = \bot$, and $\delta = \ominus$. By (ST$_{\#}$-Bot), $\mathrm{F}_1;\rho \vdash T_2 <: T_1$. By (TN-Bot), $T_2$ **nosel** $y_2$. By (TR$^{\mathrm{m}}$-Bot), $T_2 \longmapsto_{\ominus}^{\mathrm{e}} T_2$.
- Case (TR$^{\mathrm{m}}$-And): $T_1 = T_3 \wedge T_4$, and $T_2 = T_5 \wedge T_6$, and $T_3 \longmapsto_{\delta}^{\mathrm{m}} T_5$, and $T_4 \longmapsto_{\delta}^{\mathrm{m}} T_6$. By inversion of (TN-And), $T_3$ **nosel** $y_2$, and $T_4$ **nosel** $y_2$.

  - If $\delta = \oplus$, then by induction, $\mathrm{F}_1;\rho \vdash T_3 <: T_5$, and $\mathrm{F}_1;\rho \vdash T_4 <: T_6$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto_{\delta}^{\mathrm{e}} T_5$, and $T_6 \longmapsto_{\delta}^{\mathrm{e}} T_6$. By 5.18(AndSub), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$.
  - Otherwise, $\delta = \ominus$. By induction, $\mathrm{F}_1;\rho \vdash T_5 <: T_3$, and $\mathrm{F}_1;\rho \vdash T_6 <: T_4$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto_{\delta}^{\mathrm{e}} T_5$, and $T_6 \longmapsto_{\delta}^{\mathrm{e}} T_6$. By 5.18(AndSub), $\mathrm{F}_1;\rho \vdash T_2 <: T_1$.

  By (TN-And), $T_2$ **nosel** $y_2$. By (TER-And), $T_2 \longmapsto_{\delta}^{\mathrm{e}} T_2$.
- Case (TR$^{\mathrm{m}}$-Or): $T_1 = T_3 \vee T_4$, and $T_2 = T_5 \vee T_6$, and $T_3 \longmapsto_{\delta}^{\mathrm{m}} T_5$, and $T_4 \longmapsto_{\delta}^{\mathrm{m}} T_6$. By inversion of (TN-Or), $T_3$ **nosel** $y_2$, and $T_4$ **nosel** $y_2$.

  - If $\delta = \oplus$, then by induction, $\mathrm{F}_1;\rho \vdash T_3 <: T_5$, and $\mathrm{F}_1;\rho \vdash T_4 <: T_6$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto_{\delta}^{\mathrm{e}} T_5$, and $T_6 \longmapsto_{\delta}^{\mathrm{e}} T_6$. By 5.19(OrSub), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$.
  - Otherwise, $\delta = \ominus$. By induction, $\mathrm{F}_1;\rho \vdash T_5 <: T_3$, and $\mathrm{F}_1;\rho \vdash T_6 <: T_4$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto_{\delta}^{\mathrm{e}} T_5$, and $T_6 \longmapsto_{\delta}^{\mathrm{e}} T_6$. By 5.19(OrSub), $\mathrm{F}_1;\rho \vdash T_2 <: T_1$.

  By (TN-Or), $T_2$ **nosel** $y_2$. By (TER-Or), $T_2 \longmapsto_{\delta}^{\mathrm{e}} T_2$.

- Case (TR$^{\mathrm{m}}$-Fld): $T_1 = \{a : T_3..T_4\}$, and $T_2 = \{a : T_5..T_6\}$, and $T_3 \longmapsto^{\mathrm{m}}_{-\delta} T_5$, and $T_4 \longmapsto^{\mathrm{m}}_{\delta} T_6$. By inversion of (TN-Fld), $T_3$ **nosel** $y_2$, and $T_4$ **nosel** $y_2$.
  - If $\delta = \oplus$, then by induction, $\mathrm{F}_1;\rho \vdash T_5 <: T_3$, and $\mathrm{F}_1;\rho \vdash T_4 <: T_6$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_5$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_6$. By (ST-Fld), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$.
  - Otherwise, $\delta = \ominus$. By induction, $\mathrm{F}_1;\rho \vdash T_3 <: T_5$, and $\mathrm{F}_1;\rho \vdash T_6 <: T_4$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_5$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_6$. By (ST-Fld), $\mathrm{F}_1;\rho \vdash T_2 <: T_1$.

  By (TN-Fld), $T_2$ **nosel** $y_2$. By (TER-Fld), $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_2$.
- Case (TR$^{\mathrm{m}}$-Typ): $T_1 = \{B(r) : T_3..T_4\}$, and $T_2 = \{B(r) : T_5..T_6\}$, and $T_3 \longmapsto^{\mathrm{m}}_{-\delta} T_5$, and $T_4 \longmapsto^{\mathrm{m}}_{\delta} T_6$. By inversion of (TN-Typ), $T_3$ **nosel** $y_2$, and $T_4$ **nosel** $y_2$.
  - If $\delta = \oplus$, then by induction, $\mathrm{F}_1;\rho \vdash T_5 <: T_3$, and $\mathrm{F}_1;\rho \vdash T_4 <: T_6$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_5$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_6$. By (ST-Typ), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$.
  - Otherwise, $\delta = \ominus$. By induction, $\mathrm{F}_1;\rho \vdash T_3 <: T_5$, and $\mathrm{F}_1;\rho \vdash T_6 <: T_4$, and $T_5$ **nosel** $y_2$, and $T_6$ **nosel** $y_2$, and $T_5 \longmapsto^{\mathrm{e}}_{-\delta} T_5$, and $T_6 \longmapsto^{\mathrm{e}}_{\delta} T_6$. By (ST-Typ), $\mathrm{F}_1;\rho \vdash T_2 <: T_1$.

  By (TN-Typ), $T_2$ **nosel** $y_2$. By (TER-Typ), $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_2$.
- Case (TR$^{\mathrm{m}}$-MetU): $T_2 = \top$, and $\delta = \oplus$. By (ST-Top), $\mathrm{F}_1;\rho \vdash T_1 <: T_2$. By (TN-Top), $T_2$ **nosel** $y_2$. By (TER-Top), $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_2$.
- Case (TR$^{\mathrm{m}}$-MetL): $T_2 = \bot$, and $\delta = \ominus$. By (ST-Bot), $\mathrm{F}_1;\rho \vdash T_2 <: T_1$. By (TN-Bot), $T_2$ **nosel** $y_2$. By (TER-Bot), $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_2$.

□

**Lemma 5.115** (TSubCut). *If* $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_3$, *and* $T_3$ **nosel** $y_2$, *and* $\mathrm{F}_2 = \mathrm{F}_1, y_2 : T$, *and* $\mathrm{F}_2;\rho \vdash^{\mathrm{m}}_{\oplus} T_1 <: T_2$, *and* $y_2 \notin \mathrm{fv}\ \mathrm{F}_1$, *then there exists* $T_4$, *such that* $\mathrm{F}_1;\rho \vdash T_3 <: T_4$, *and* $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$, *and* $T_4$ **nosel** $y_2$. *If* $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_6$, *and* $T_6$ **nosel** $y_2$, *and* $\mathrm{F}_2 = \mathrm{F}_1, y_2 : T$, *and* $y_2 \notin \mathrm{fv}\ \mathrm{F}_1$, *and* $\mathrm{F}_2;\rho \vdash^{\mathrm{m}}_{\ominus} T_1 <: T_2$, *then there exists* $T_5$, *such that* $\mathrm{F}_1;\rho \vdash T_5 <: T_6$, *and* $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_5$, *and* $T_1$ **nosel** $y_2$.

*Idea.* Method-free subtyping does not use variables which are not in the type. ▽

*Proof idea.* Induction on method-free subtyping. ▽

*Proof.* Induction on $\mathrm{F}_2;\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_2$:

- Case (ST$^{\mathrm{m}}_{\#}$-Top): $T_2 = \top$.
  - If $\delta = \oplus$, then choose $T_4 = \top$. By (TN-Top), $T_4$ **nosel** $y_2$. By (TER-Top), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By (ST-Top), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By inversion of (TER-Top), $T_6 = \top$. By 5.103(ERedEx), exists $T_5$, such that $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_5$, and $T_5$ **nosel** $y_2$. By (ST-Top), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.
- Case (ST$^{\mathrm{m}}_{\#}$-Bot): $T_1 = \bot$, $\mathrm{F}_1;\rho \vdash \bot <: T_2$.
  - If $\delta = \ominus$, then choose $T_5 = \bot$. By (TN-Bot), $T_5$ **nosel** $y_2$. By (TER-Bot), $T_1 \longmapsto^{\mathrm{e}}_{\oplus} T_5$. By (ST-Bot), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.
  - Otherwise, $\delta = \oplus$. By inversion of (TER-Bot), $T_3 = \bot$. By 5.103(ERedEx), exists $T_4$, such that $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$, and $T_4$ **nosel** $y_2$. By (ST-Bot), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$.
- Case (ST$^{\mathrm{m}}_{\#}$-Refl): $T_1 = T_2$.
  - If $\delta = \oplus$. Choose $T_4 = T_3$. By (ST-Refl), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. Trivially, $T_4$ **nosel** $y_2$.
  - Otherwise, $\delta = \ominus$. Choose $T_5 = T_6$. By (ST-Refl), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. Trivially, $T_5$ **nosel** $y_2$.
- Case (ST$^{\mathrm{m}}_{\#}$-N-Rec): $T_1 = \mathsf{N}$, and $T_2 = \mu(s : T_7)$.
  - If $\delta = \oplus$, then by inversion of (TER-N), $T_3 = \mathsf{N}$. Choose $T_4 = T_2$. By (TER-Rec), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By (ST-N-Rec), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TN-Rec), $T_4$ **nosel** $y_2$.
  - Otherwise, $\delta = \ominus$, then by inversion of (TER-Rec), $T_6 = \mu(s : T_7)$. Choose $T_5 = \bot$. By (TER-N-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST-Bot), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\ominus} T_5 <: T_6$. By (TN-Bot), $T_5$ **nosel** $y_2$.

- Case (ST$^{\mathrm{m}}_{\#}$-N-M): $T_1 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_2 = \bot$.
  - If $\delta = \oplus$, then by inversion of (TER-And), and by inversion of (TER-N) and 5.101(ERedMut), $T_3 = T_1$. Choose $T_4 = T_2$. By (TER-Bot), $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_4$. By (ST-N-M), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TN-Bot), $T_4$ **nosel** $y_2$.
  - Otherwise, $\delta = \ominus$, then by inversion of (TER-Bot), $T_6 = T_2$. Choose $T_5 = \bot \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By (TER-Bot) and (TER-Typ) and (TER-N-Bot) and (TER-And), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST-N-M), $\mathrm{F}_1;\rho \vdash \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\} <: T_6$. By (ST-Bot) and (ST-Refl) and 5.18(AndSub), $\mathrm{F}_1;\rho \vdash T_5 <: \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.

- Case (ST$^{\mathrm{m}}_{\#}$-And1): $T_1 = T_2 \wedge T_7$.
  - If $\delta = \oplus$. By inversion of (TER-And), $T_3 = T_8 \wedge T_9$, such that $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$. By inversion of (TN-And), $T_8$ **nosel** $y_2$. Choose $T_4 = T_8$. By (ST-And1), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By 5.103(ERedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_8$ **nosel** $y_2$. Choose $T_5 = T_6 \wedge T_8$. By (TN-And), $T_5$ **nosel** $y_2$. By (TER-And), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_5$. By (ST-And1), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.

- Case (ST$^{\mathrm{m}}_{\#}$-And2): $T_1 = T_7 \wedge T_2$.
  - If $\delta = \oplus$. By inversion of (TER-And), $T_3 = T_9 \wedge T_8$, such that $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$. By inversion of (TN-And), $T_8$ **nosel** $y_2$. Choose $T_4 = T_8$. By (ST-And2), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$.
  - Otherwise, $\delta = \ominus$. By 5.103(ERedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_8$ **nosel** $y_2$. Choose $T_5 = T_8 \wedge T_6$. By (TN-And), $T_5$ **nosel** $y_2$. By (TER-And), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_5$. By (ST-And2), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.

- Case (ST$^{\mathrm{m}}_{\#}$-And): $T_2 = T_7 \wedge T_8$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_8$.
  - If $\delta = \oplus$. By induction, exists $T_9$, such that $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $\mathrm{F}_1;\rho \vdash T_3 <: T_9$, and $T_9$ **nosel** $y_2$. By induction, exists $T_{10}$, such that $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$, and $\mathrm{F}_1;\rho \vdash T_3 <: T_{10}$, and $T_{10}$ **nosel** $y_2$. Choose $T_4 = T_9 \wedge T_{10}$. By (TER-And), $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-And), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TN-And), $T_4$ **nosel** $y_2$.
  - Otherwise, $\delta = \ominus$. By inversion of (TER-And), exist $T_9$, $T_{10}$, such that $T_6 = T_9 \wedge T_{10}$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By inversion of (TN-And), $T_9$ **nosel** $y_2$, and $T_{10}$ **nosel** $y_2$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F}_1;\rho \vdash T_{11} <: T_9$, and $\mathrm{F}_1;\rho \vdash T_{12} <: T_{10}$, and $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $T_{11}$ **nosel** $y_2$, and $T_{12}$ **nosel** $y_2$. By 5.105(ERedCom), exists $T_5$, such that $T_5$ **nosel** $y_2$, and $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_5$, and $\mathrm{F}_1;\rho \vdash T_5 <: T_{11}$, and $\mathrm{F}_1;\rho \vdash T_5 <: T_{12}$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_5 <: T_9$, and $\mathrm{F}_1;\rho \vdash T_5 <: T_{10}$. By (ST-And), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.

- Case (ST$^{\mathrm{m}}_{\#}$-Or1): $T_2 = T_1 \vee T_7$.
  - If $\delta = \ominus$. By inversion of (TER-Or), $T_6 = T_8 \vee T_9$, such that $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$. By inversion of (TN-Or), $T_8$ **nosel** $y_2$. Choose $T_5 = T_8$. By (ST-Or1), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.
  - Otherwise, $\delta = \oplus$. By 5.103(ERedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_8$ **nosel** $y_2$. Choose $T_4 = T_3 \vee T_8$. By (TN-Or), $T_4$ **nosel** $y_2$. By (TER-Or), $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Or1), $\mathrm{F}_1;\rho \vdash T_3 <: T_5$.

- Case (ST$^{\mathrm{m}}_{\#}$-Or2): $T_2 = T_7 \vee T_1$.
  - If $\delta = \ominus$. By inversion of (TER-Or), $T_6 = T_9 \vee T_8$, such that $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$. By inversion of (TN-Or), $T_8$ **nosel** $y_2$. Choose $T_5 = T_8$. By (ST-Or2), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.
  - Otherwise, $\delta = \oplus$. By 5.103(ERedEx), exists $T_8$, such that $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_8$ **nosel** $y_2$. Choose $T_4 = T_8 \vee T_3$. By (TN-Or), $T_4$ **nosel** $y_2$. By (TER-Or), $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Or2), $\mathrm{F}_1;\rho \vdash T_3 <: T_5$.

- Case (ST$^{\mathrm{m}}_{\#}$-Or): $T_1 = T_7 \vee T_8$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_7 <: T_2$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_8 <: T_2$.
  - If $\delta = \ominus$. By induction, exists $T_9$, such that $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $\mathrm{F}_1;\rho \vdash T_9 <: T_6$, and $T_9$ **nosel** $y_2$. By induction, exists $T_{10}$, such that $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$, and $\mathrm{F}_1;\rho \vdash T_{10} <: T_6$, and $T_{10}$ **nosel** $y_2$. Choose $T_5 = T_9 \vee T_{10}$. By (TER-Or), $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_5$. By (ST-Or), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. By (TN-Or), $T_5$ **nosel** $y_2$.

  - Otherwise, $\delta = \oplus$. By inversion of (TER-Or), exist $T_9$, $T_{10}$, such that $T_3 = T_9 \vee T_{10}$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_9$, and $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$. By inversion of (TN-Or), $T_9$ **nosel** $y_2$, and $T_{10}$ **nosel** $y_2$. By induction, exist $T_{11}$, $T_{12}$, such that $\mathrm{F}_1;\rho \vdash T_9 <: T_{11}$, and $\mathrm{F}_1;\rho \vdash T_{10} <: T_{12}$, and $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, and $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, and $T_{11}$ **nosel** $y_2$, and $T_{12}$ **nosel** $y_2$. By 5.105(ERedCom), exists $T_4$, such that $T_4$ **nosel** $y_2$, and $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$, and $\mathrm{F}_1;\rho \vdash T_{11} <: T_4$, and $\mathrm{F}_1;\rho \vdash T_{12} <: T_4$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_9 <: T_4$, and $\mathrm{F}_1;\rho \vdash T_{10} <: T_4$. By (ST-Or), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$.

- Case (ST$^{\mathrm{m}}_{\#}$-Trans): $\mathrm{F}_2;\rho \vdash^{\mathrm{m}}_{\delta} T_1 <: T_7$, and $\mathrm{F}_2;\rho \vdash^{\mathrm{m}}_{\delta} T_7 <: T_2$. If $\delta = \oplus$, then by induction, exists $T_8$, such that $\mathrm{F}_1;\rho \vdash T_3 <: T_8$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_8$ **nosel** $y_2$. By induction, exists $T_4$, such that $\mathrm{F}_1;\rho \vdash T_8 <: T_4$, and $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$, and $T_4$ **nosel** $y_2$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. If $\delta = \ominus$, then by induction, exists $T_8$, such that $\mathrm{F}_1;\rho \vdash T_8 <: T_6$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_8$, and $T_8$ **nosel** $y_2$. By induction, exists $T_5$, such that $\mathrm{F}_1;\rho \vdash T_5 <: T_8$, and $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_5$, and $T_5$ **nosel** $y_2$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.

- Case (ST$^{\mathrm{m}}_{\#}$-SelL): $\delta = \ominus$. $\mathrm{F}_2 \vdash_! v : \{B(r) : T_7..T_8\}$, and $T_2 = v.B(x_2)$, and $[x_2/r]T_7 \longmapsto^{\mathrm{m}}_{\ominus} T_1$. By inversion of (TN-Sel), $v \neq y_2$, and $x_2 \neq y_2$. By 5.110(PrecCut), $\mathrm{F}_1 \vdash_! v : \{B(r) : T_7..T_8\}$. By 5.78(VTEqB), $\mathrm{F}_1;\rho \vdash v : \{B(r) : T_7..T_8\}$. By inversion:

  - Case (TER-Sel): $T_2 = T_6$. By (ST-SelL), $\mathrm{F}_1;\rho \vdash [x_2/r]T_7 <: T_6$. Choose $T_5 = T_1$. By 5.111(PrecFV), $y_2 \notin \mathrm{fv}\ T_7$. By 5.112(NoselFV), $T_7$ **nosel** $y_2$. By 5.113(NoselSub), $[x_2/r]T_7$ **nosel** $y_2$. By 5.114(TRedCut), $\mathrm{F}_1;\rho \vdash T_5 <: [x_2/r]T_7$, and $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_5$, and $T_5$ **nosel** $y_2$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.
  - Case (TER-SelL): $T_6 = \top$. By 5.103(ERedEx), exists $T_5$, such that $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_5$, and $T_5$ **nosel** $y_2$. By (ST-Top), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$.

- Case (ST$^{\mathrm{m}}_{\#}$-SelU): $\delta = \oplus$. $\mathrm{F}_2 \vdash_! v : \{B(r) : T_7..T_8\}$, and $T_1 = v.B(x_2)$, and $[x_2/r]T_8 \longmapsto^{\mathrm{m}}_{\oplus} T_2$. By inversion of (TN-Sel), $v \neq y_2$, and $x_2 \neq y_2$. By 5.110(PrecCut), $\mathrm{F}_1 \vdash_! v : \{B(r) : T_7..T_8\}$. By 5.78(VTEqB), $\mathrm{F}_1;\rho \vdash v : \{B(r) : T_7..T_8\}$. By inversion:

  - Case (TER-Sel): $T_1 = T_3$. By (ST-SelU), $\mathrm{F}_1;\rho \vdash T_1 <: [x_2/r]T_8$. Choose $T_4 = T_2$. By 5.111(PrecFV), $y_2 \notin \mathrm{fv}\ T_8$. By 5.112(NoselFV), $T_8$ **nosel** $y_2$. By 5.113(NoselSub), $[x_2/r]T_8$ **nosel** $y_2$. By 5.114(TRedCut), $\mathrm{F}_1;\rho \vdash [x_2/r]T_8 <: T_4$, and $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$, and $T_4$ **nosel** $y_2$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$.
  - Case (TER-SelU): $T_3 = \bot$. By 5.103(ERedEx), exists $T_4$, such that $T_2 \longmapsto^{\mathrm{e}}_{\ominus} T_4$, and $T_4$ **nosel** $y_2$. By (ST-Bot), $\mathrm{F};\rho \vdash^{\mathrm{m}}_{T_4} T_3 <: \mathrm{F}_1$.

- Case (ST$^{\mathrm{m}}_{\#}$-Typ): $T_1 = \{B(r) : T_7..T_8\}$, and $T_2 = \{B(r) : T_9..T_{10}\}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{-\delta} T_9 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_8 <: T_{10}$.

  - If $\delta = \oplus$. By inversion of (TER-Typ), $T_3 = \{B(r) : T_{11}..T_{12}\}$, where $T_7 \longmapsto^{\mathrm{e}}_{\ominus} T_{11}$, and $T_8 \longmapsto^{\mathrm{e}}_{\oplus} T_{12}$. By inversion of (TN-Typ), $T_{11}$ **nosel** $y_2$, and $T_{12}$ **nosel** $y_2$. By induction, exist $T_{13}$, $T_{14}$, such that $T_9 \longmapsto^{\mathrm{e}}_{\ominus} T_{13}$, and $\mathrm{F}_1;\rho \vdash T_{13} <: T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\oplus} T_{14}$, and $\mathrm{F}_1;\rho \vdash T_{12} <: T_{14}$, and $T_{13}$ **nosel** $y_2$, and $T_{14}$ **nosel** $y_2$. Choose $T_4 = \{B(r) : T_{13}..T_{14}\}$. By (TER-Typ), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By (ST-Typ), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TN-Typ), $T_4$ **nosel** $y_2$.
  - Otherwise, $\delta = \ominus$. By inversion of (TER-Typ), $T_6 = \{B(r) : T_{11}..T_{12}\}$, where $T_9 \longmapsto^{\mathrm{e}}_{\oplus} T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\ominus} T_{12}$. By inversion of (TN-Typ), $T_{11}$ **nosel** $y_2$, and $T_{12}$ **nosel** $y_2$. By induction, exist $T_{13}$, $T_{14}$, such that $T_7 \longmapsto^{\mathrm{e}}_{\oplus} T_{13}$, and $\mathrm{F}_1;\rho \vdash T_{11} <: T_{13}$, and $T_8 \longmapsto^{\mathrm{e}}_{\ominus} T_{14}$, and $\mathrm{F}_1;\rho \vdash T_{14} <: T_{12}$, and $T_{13}$ **nosel** $y_2$, and $T_{14}$ **nosel** $y_2$. Choose $T_5 = \{B(r) : T_{13}..T_{14}\}$. By (TER-Typ), $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_5$. By (ST-Typ), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. By (TN-Typ), $T_5$ **nosel** $y_2$.

- Case (ST$^{\mathrm{m}}_{\#}$-Fld): $T_1 = \{a : T_7..T_8\}$, and $T_2 = \{a : T_9..T_{10}\}$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{-\delta} T_9 <: T_7$, and $\mathrm{F};\rho \vdash^{\mathrm{m}}_{\delta} T_8 <: T_{10}$.

  - If $\delta = \oplus$. By inversion of (TER-Fld), $T_3 = \{a : T_{11}..T_{12}\}$, where $T_7 \longmapsto^{\mathrm{e}}_{\ominus} T_{11}$, and $T_8 \longmapsto^{\mathrm{e}}_{\oplus} T_{12}$. By inversion of (TN-Fld), $T_{11}$ **nosel** $y_2$, and $T_{12}$ **nosel** $y_2$. By induction, exist $T_{13}$, $T_{14}$, such that $T_9 \longmapsto^{\mathrm{e}}_{\ominus} T_{13}$, and $\mathrm{F}_1;\rho \vdash T_{13} <: T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\oplus} T_{14}$, and $\mathrm{F}_1;\rho \vdash T_{12} <: T_{14}$, and $T_{13}$ **nosel** $y_2$, and $T_{14}$ **nosel** $y_2$. Choose $T_4 = \{a : T_{13}..T_{14}\}$. By (TER-Fld), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By (ST-Fld), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TN-Fld), $T_4$ **nosel** $y_2$.

  - Otherwise, $\delta = \ominus$. By inversion of (TER-Fld), $T_6 = \{a : T_{11}..T_{12}\}$, where $T_9 \longmapsto^{\mathrm{e}}_{\oplus} T_{11}$, and $T_{10} \longmapsto^{\mathrm{e}}_{\ominus} T_{12}$. By inversion of (TN-Fld), $T_{11}$ $\mathbf{nosel}$ $y_2$, and $T_{12}$ $\mathbf{nosel}$ $y_2$. By induction, exist $T_{13}$, $T_{14}$, such that $T_7 \longmapsto^{\mathrm{e}}_{\oplus} T_{13}$, and $\mathrm{F}_1;\rho \vdash T_{11} <: T_{13}$, and $T_8 \longmapsto^{\mathrm{e}}_{\ominus} T_{14}$, and $\mathrm{F}_1;\rho \vdash T_{14} <: T_{12}$, and $T_{13}$ $\mathbf{nosel}$ $y_2$, and $T_{14}$ $\mathbf{nosel}$ $y_2$. Choose $T_5 = \{a : T_{13}..T_{14}\}$. By (TER-Fld), $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_5$. By (ST-Fld), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. By (TN-Fld), $T_5$ $\mathbf{nosel}$ $y_2$.

- Case ($\mathrm{ST}^{\mathrm{m}}_{\#}$-TypAnd): $T_1 = \{B(r) : T_7..T_8\} \wedge \{B(r) : T_9..T_{10}\}$, and $T_2 = \{B(r) : T_7 \vee T_9..T_8 \wedge T_{10}\}$.

  - If $\delta = \oplus$, then by inversion of (TER-And), and by inversion of (TER-Typ), $T_3 = \{B(r) : T_{11}..T_{12}\} \wedge \{B(r) : T_{13}..T_{14}\}$, where $T_7 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, where $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, where $T_9 \longmapsto^{\mathrm{e}}_{-\delta} T_{13}$, where $T_{10} \longmapsto^{\mathrm{e}}_{\delta} T_{14}$. By inversion of (TN-And), and by inversion of (TN-Typ), $\forall i \in 11, \ldots, 14$: $T_i$ $\mathbf{nosel}$ $y_2$. Choose $T_4 = \{B(r) : T_{11} \vee T_{13}..T_{12} \wedge T_{14}\}$. By (TN-And) and (TN-Or) and (TN-Typ), $T_4$ $\mathbf{nosel}$ $y_2$. By (ST-TypAnd), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TER-And) and (TER-Or) and (TER-Typ), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of (TER-Typ), and by inversion of (TER-And), and by inversion of (TER-Or), $T_6 = \{B(r) : T_{11} \vee T_{13}..T_{12} \wedge T_{14}\}$, where $T_7 \longmapsto^{\mathrm{e}}_{-\delta} T_{11}$, where $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, where $T_9 \longmapsto^{\mathrm{e}}_{-\delta} T_{13}$, where $T_{10} \longmapsto^{\mathrm{e}}_{\delta} T_{14}$. By inversion of (TN-Typ), and by inversion of (TN-And), and by inversion of (TN-Or), $\forall i \in 11, \ldots, 14$: $T_i$ $\mathbf{nosel}$ $y_2$. Choose $T_5 = \{B(r) : T_{11}..T_{12}\} \wedge \{B(r) : T_{13}..T_{14}\}$. By (TN-And) and (TN-Typ), $T_5$ $\mathbf{nosel}$ $y_2$. By (ST-TypAnd), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. By (TER-And) and (TER-Typ), $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_5$.

- Case ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Eq): $\rho \vdash T_1 \approx T_2$.

  - If $\delta = \oplus$. By 5.109(ERedEq), exists $T_4$, such that $\rho \vdash T_3 \approx T_4$, and $T_2 \longmapsto^{\mathrm{e}}_{\delta} T_4$. By (ST-Eq).
  - Otherwise, $\delta = \ominus$. By 5.2(EqSymm), $\rho \vdash T_2 \approx T_1$. By 5.109(ERedEq), exists $T_5$, such that $\rho \vdash T_6 \approx T_5$, and $T_1 \longmapsto^{\mathrm{e}}_{\delta} T_5$. By 5.2(EqSymm), $\rho \vdash T_5 \approx T_6$. By (ST-Eq).

- Case ($\mathrm{ST}^{\mathrm{m}}_{\#}$-N-Fld): $T_1 = \mathsf{N}$, and $T_2 = \{a : T_7..T_8\}$.

  - If $\delta = \oplus$, then by inversion of (TER-N), $T_3 = \mathsf{N}$. By 5.103(ERedEx), exists $T_9$, such that $T_7 \longmapsto^{\mathrm{e}}_{\ominus} T_9$, and $T_9$ $\mathbf{nosel}$ $y_2$. By 5.103(ERedEx), exists $T_{10}$, such that $T_8 \longmapsto^{\mathrm{e}}_{\oplus} T_{10}$, and $T_{10}$ $\mathbf{nosel}$ $y_2$. Choose $T_4 = \{a : T_9..T_{10}\}$. By (TER-Fld), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By (ST-N-Fld), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TN-Fld), $T_4$ $\mathbf{nosel}$ $y_2$.
  - Otherwise, $\delta = \ominus$, then by inversion of (TER-Fld), $T_6 = \{a : T_9..T_{10}\}$. Choose $T_5 = \bot$. By (TER-N-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST-Bot), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. By (TN-Bot), $T_5$ $\mathbf{nosel}$ $y_2$.

- Case ($\mathrm{ST}^{\mathrm{m}}_{\#}$-N-Typ): $T_1 = \mathsf{N}$, and $T_2 = \{A(r) : T_7..T_8\}$.

  - If $\delta = \oplus$, then by inversion of (TER-N), $T_3 = \mathsf{N}$. By 5.103(ERedEx), exists $T_9$, such that $T_7 \longmapsto^{\mathrm{e}}_{\ominus} T_9$, and $T_9$ $\mathbf{nosel}$ $y_2$. By 5.103(ERedEx), exists $T_{10}$, such that $T_8 \longmapsto^{\mathrm{e}}_{\oplus} T_{10}$, and $T_{10}$ $\mathbf{nosel}$ $y_2$. Choose $T_4 = \{A(r) : T_9..T_{10}\}$. By (TER-Typ), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$. By (ST-N-Typ), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TN-Typ), $T_4$ $\mathbf{nosel}$ $y_2$.
  - Otherwise, $\delta = \ominus$, then by inversion of (TER-Typ), $T_6 = \{A(r) : T_9..T_{10}\}$. Choose $T_5 = \bot$. By (TER-N-Bot), $T_1 \longmapsto^{\mathrm{m}}_{\ominus} T_5$. By (ST-Bot), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. By (TN-Bot), $T_5$ $\mathbf{nosel}$ $y_2$.

- Case ($\mathrm{ST}^{\mathrm{m}}_{\#}$-Dist): $T_1 = T_7 \wedge (T_8 \vee T_9)$. $T_2 = (T_7 \wedge T_8) \vee (T_7 \wedge T_9)$.

  - If $\delta = \oplus$, then by inversion of (TER-And), and by inversion of (TER-Or), $T_3 = T_{10} \wedge (T_{11} \vee T_{12})$, where $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$, where $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, where $T_9 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$. By inversion of (TN-And), and by inversion of (TN-Or), $\forall i \in 10, \ldots, 12$: $T_i$ $\mathbf{nosel}$ $y_2$. Choose $T_4 = (T_{10} \wedge T_{11}) \vee (T_{10} \wedge T_{12})$. By (TN-And) and (TN-Or), $T_4$ $\mathbf{nosel}$ $y_2$. By (ST-Dist), $\mathrm{F}_1;\rho \vdash T_3 <: T_4$. By (TER-And) and (TER-Or), $T_2 \longmapsto^{\mathrm{e}}_{\oplus} T_4$.
  - Otherwise, $\delta = \ominus$, then by inversion of (TER-Or), and by inversion of (TER-And), $T_6 = (T_{11} \wedge T_{13}) \vee (T_{12} \wedge T_{14})$, where $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_{11}$, where $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_{12}$, where $T_8 \longmapsto^{\mathrm{e}}_{\delta} T_{13}$, where $T_9 \longmapsto^{\mathrm{e}}_{\delta} T_{14}$. By inversion of (TN-Or), and by inversion of (TN-And), $\forall i \in 11, \ldots, 14$: $T_i$ $\mathbf{nosel}$ $y_2$. By 5.105(ERedCom), exists $T_{10}$, such that $T_{10}$ $\mathbf{nosel}$ $y_2$, and $T_7 \longmapsto^{\mathrm{e}}_{\delta} T_{10}$, and $\mathrm{F}_1;\rho \vdash T_{10} <: T_{11}$, and $\mathrm{F}_1;\rho \vdash T_{10} <: T_{12}$. Choose $T_5 = T_{10} \wedge (T_{13} \vee T_{14})$. By (TN-Or) and (TN-And), $T_5$ $\mathbf{nosel}$ $y_2$. By (ST-TypAnd), $\mathrm{F}_1;\rho \vdash T_5 <: (T_{10} \wedge T_{13}) \vee (T_{10} \wedge T_{14})$. By 5.18(AndSub) and 5.19(OrSub) and (ST-Trans), $\mathrm{F}_1;\rho \vdash T_5 <: T_6$. By (TER-Or) and (TER-And), $T_1 \longmapsto^{\mathrm{e}}_{\ominus} T_5$.

□

**Lemma 5.116** (FromSSub). *If* $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_2$*, then* $\mathrm{F};\rho \vdash T_1 <: T_2$*.*

*Proof.* Induction on $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_2$:

- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Top): $T_2 = \top$. Directly by (ST-Top).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Bot): $T_1 = \bot$. Directly by (ST-Bot).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Refl): $T_1 = T_2$. Directly by (ST-Refl).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-And1): $T_1 = T_2 \wedge T_4$. By (ST-And1), $\mathrm{F};\rho \vdash T_4 \wedge T_2 <: T_2$.
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-And2): $T_1 = T_4 \wedge T_2$. By (ST-And2), $\mathrm{F};\rho \vdash T_4 \wedge T_2 <: T_2$.
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-And): $T_2 = T_4 \wedge T_5$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_4$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_5$. By induction on subtyping, $\mathrm{F};\rho \vdash T_1 <: T_4$, $\mathrm{F};\rho \vdash T_1 <: T_5$. By (ST-And), $\mathrm{F};\rho \vdash T_1 <: T_4 \wedge T_5$.
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Or1): $T_2 = T_1 \vee T_4$. By (ST-Or1), $\mathrm{F};\rho \vdash T_1 <: T_1 \vee T_4$.
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Or2): $T_2 = T_4 \vee T_1$. By (ST-Or2), $\mathrm{F};\rho \vdash T_1 <: T_4 \vee T_1$.
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Or): $T_1 = T_4 \vee T_5$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_4 <: T_2$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_5 <: T_2$. By induction on subtyping, $\mathrm{F};\rho \vdash T_4 <: T_2$, $\mathrm{F};\rho \vdash T_5 <: T_2$. By (ST-Or), $\mathrm{F};\rho \vdash T_4 \vee T_5 <: T_2$.
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Trans): $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_1 <: T_4$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_4 <: T_2$.

  By induction on subtyping, $\mathrm{F};\rho \vdash T_1 <: T_4$, and $\mathrm{F};\rho \vdash T_4 <: T_2$. By (ST-Trans), $\mathrm{F};\rho \vdash T_1 <: T_2$.
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-SelL): By ($\mathrm{ST}_{\#}$-SelL) and 5.78(VTEqB).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-SelU): By ($\mathrm{ST}_{\#}$-SelU) and 5.78(VTEqB).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-TypAnd): $T_1 = \{B(r) : T_4..T_5\} \wedge \{B(r) : T_6..T_7\}$, and $T_2 = \{B(r) : T_4 \vee T_6..T_5 \wedge T_7\}$. By (ST-TypAnd).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Dist): $T_1 = T_4 \wedge (T_5 \vee T_6)$. $T_2 = (T_4 \wedge T_5) \vee (T_4 \wedge T_6)$. By (ST-Dist).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Typ): $T_1 = \{B(r) : T_4..T_5\}$, and $T_2 = \{B(r) : T_6..T_7\}$, where $\mathrm{F};\rho \vdash^{\mathsf{s}}_{-\delta} T_6 <: T_4$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_5 <: T_7$.

  By induction on subtyping, $\mathrm{F};\rho \vdash T_6 <: T_4$, and $\mathrm{F};\rho \vdash T_5 <: T_7$. By (ST-Typ).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Fld): $T_1 = \{a : T_4..T_5\}$, and $T_2 = \{a : T_6..T_7\}$, where $\mathrm{F};\rho \vdash^{\mathsf{s}}_{-\delta} T_6 <: T_4$, and $\mathrm{F};\rho \vdash^{\mathsf{s}}_{\delta} T_5 <: T_7$.

  By induction on subtyping, $\mathrm{F};\rho \vdash T_6 <: T_4$, and $\mathrm{F};\rho \vdash T_5 <: T_7$. By (ST-Fld).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Met): $T_1 = \{m(z : T_4, r : T_6) : T_5\}$, and $T_2 = \{m(z : T_7, r : T_9) : T_8\}$, where $\mathrm{F};\rho \vdash_{\#} T_7 <: T_4$, and $\mathrm{F}, z : T_7;\rho \vdash T_9 <: T_6$, and $\mathrm{F}, z : T_7, r : T_9;\rho \vdash T_5 <: T_8$.

  By 5.78(VTEqB), $\mathrm{F};\rho \vdash T_7 <: T_4$. By (ST-Met).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-Eq): By (ST-Eq).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-N-M): $T_1 = \mathsf{N} \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $T_2 = \bot$. By (ST-N-M).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-N-Rec): $T_1 = \mathsf{N}$, and $T_2 = \mu(s : T_4)$. By (ST-N-Rec).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-N-Fld): $T_1 = \mathsf{N}$, and $T_2 = \{a : T_6..T_7\}$. By (ST-N-Fld).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-N-Met): $T_1 = \mathsf{N}$, and $T_2 = \{m(z : T_7, r : T_9) : T_8\}$. By (ST-N-Met).
- Case ($\mathrm{ST}^{\mathsf{s}}_{\#}$-N-Typ): $T_1 = \mathsf{N}$, and $T_2 = \{B(r) : T_6..T_7\}$. By (ST-N-Typ).

□

**Lemma 5.117** (StnMRef). *If* $v_1 \neq w_2$*, and* $\mathrm{F}_2 = \mathrm{F}_1, w_2 : T$*, and* $\rho_2 = \rho_1, w_2 \to y_2$*, and* $\mathrm{F}_2 \sim \rho_2$*, and* $\mathrm{F}_2;\rho_2 \vdash v_1 : \{\mathsf{M}(r_0) : \bot..\bot\}$*, then* $\mathrm{F}_1;\rho_1 \vdash v_1 : \{\mathsf{M}(r_0) : \bot..\bot\}$*.*

*Idea.* Adding a new reference to the context and environment cannot cause existing references to become mutable. ▽

*Proof idea.* Substitute $y_2$ for $w_2$. ▽

*Proof.* Because references in $\rho_2$ are unique, $w_2 \notin \rho_1$. By 5.32(SubW), $\mathrm{F}_1;\rho_1 \vdash [y_2/w_2]v_1 : [y_2/w_2]\{\mathsf{M}(r_0) : \bot..\bot\}$. By (VX-VarN), $[y_2/w_2]v_1 = v_1$. By (TX-Bot) and (TX-Typ), $[y_2/w_2]\{\mathsf{M}(r_0) : \bot..\bot\} = \{\mathsf{M}(r_0) : \bot..\bot\}$. □

**Lemma 5.118** (StnSubBot). *If* $\mathrm{F}_2 = \mathrm{F}_1, y_2 : T$*, and* $\mathrm{F}_2;\rho \vdash_{\#} T_4 <: \bot$*, and* $T_4$ **nosel** $y_2$*, then* $\mathrm{F}_1;\rho \vdash T_4 <: \bot$.

*Proof.* By 5.99(ToSRed), exist $T_5$, $T_6$, such that $\mathrm{F}_2 \vdash T_4 \longmapsto^{\mathrm{s}}_{\oplus} T_5$, and $\mathrm{F}_2 \vdash \bot \longmapsto^{\mathrm{s}}_{\oplus} T_6$, and $\mathrm{F}_2;\rho \vdash^{\mathrm{s}}_{\oplus} T_5 <: T_6$. By 5.93(SRedInv), $T_6 = \bot$. By 5.92(SRedSub), $\mathrm{F}_2;\rho \vdash^{\mathrm{s}}_{\oplus} T_4 <: T_5$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F}_2;\rho \vdash^{\mathrm{s}}_{\oplus} T_4 <: \bot$. By 5.108(ToTRed), exist $T_7$, $T_8$, such that $T_4 \longmapsto^{\mathrm{m}}_{\oplus} T_7$, and $\bot \longmapsto^{\mathrm{m}}_{\oplus} T_8$, and $\mathrm{F}_2;\rho \vdash^{\mathrm{m}}_{\oplus} T_7 <: T_8$. By inversion of ($\mathrm{TR}^{\mathrm{m}}$-Bot), $T_8 = \bot$. By 5.114(TRedCut), $\mathrm{F}_1;\rho \vdash T_4 <: T_7$, and $T_7$ **nosel** $y_2$, and $T_7 \longmapsto^{\mathrm{e}}_{\oplus} T_7$. By 5.115(TSubCut), exists $T_9$, such that $\bot \longmapsto^{\mathrm{e}}_{\oplus} T_9$, and $\mathrm{F}_1;\rho \vdash T_7 <: T_9$. By inversion of (TER-Bot), $T_9 = \bot$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_4 <: \bot$. □

**Lemma 5.119** (StnMLoc). *If* $v_1 \neq y_2$*, and* $\mathrm{F}_2 = \mathrm{F}_1, y_2 : T$*, and* $\mathrm{F}_2;\rho \vdash v_1 : \{\mathsf{M}(r_0) : \bot..\bot\}$*, then* $\mathrm{F}_1;\rho \vdash v_1 : \{\mathsf{M}(r_0) : \bot..\bot\}$.

*Idea.* Adding a new location to the context cannot cause existing references to become mutable. ▽

*Proof idea.* The mutability must come from the context type of $v_1$. ▽

*Proof.* By 5.77(VTEq), $\mathrm{F}_2;\rho_2 \vdash_{\#\#} v_1 : \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.60(InvT), $\mathrm{F}_2 \vdash_{!} v_1 : \{\mathsf{M}(r_0) : T_1..T_2\}$, and $\mathrm{F}_2;\rho_2 \vdash_{\#} \bot <: T_1$, and $\mathrm{F}_2;\rho_2 \vdash_{\#} T_2 <: \bot$. By 5.110(PrecCut), $\mathrm{F}_1 \vdash_{!} v_1 : \{\mathsf{M}(r_0) : T_1..T_2\}$. By 5.111(PrecFV), $y_2 \notin \mathrm{fv}\ T_2$. By 5.112(NoselFV), $T_2$ **nosel** $y_2$. By 5.118(StnSubBot), $\mathrm{F}_1;\rho \vdash T_2 <: \bot$. By (ST-Typ), $\mathrm{F}_1;\rho \vdash \{\mathsf{M}(r_0) : T_1..T_2\} <: \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.78(VTEqB), $\mathrm{F}_1;\rho \vdash v_1 : \{\mathsf{M}(r_0) : T_1..T_2\}$. By (VT-Sub), $\mathrm{F}_1;\rho \vdash v_1 : \{\mathsf{M}(r_0) : \bot..\bot\}$. □

**Lemma 5.120** (StnMFRef). *If* $y_1 \neq w_2$*, and* $\mathrm{F}_2 = \mathrm{F}_1, w_2 : T$*, and* $\rho_2 = \rho_1, w_2 \to y_2$*, and* $\mathrm{F}_2 \sim \rho_2$*, and* $\mathrm{F}_2;\rho_2 \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$*, then* $\mathrm{F}_1;\rho_1 \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$.

*Idea.* Adding a new reference to the context and environment cannot cause existing fields to become mutable. ▽

*Proof idea.* Substitute $y_2$ for $w_2$. ▽

*Proof.* Because references in $\rho_2$ are unique, $w_2 \notin \rho_1$. By 5.32(SubW), $\mathrm{F}_1;\rho_1 \vdash [y_2/w_2]y_1 : [y_2/w_2]\{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By (VX-VarN), $[y_2/w_2]y_1 = y_1$. By (TX-Bot) and (TX-Typ) and (TX-Fld), $[y_2/w_2]\{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\} = \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. □

**Lemma 5.121** (StnSub). *If* $\mathrm{F}_2 = \mathrm{F}_1, y_2 : T_1$*, and* $\mathrm{F}_2;\rho \vdash_{\#} T_2 <: \{\mathsf{M}(r_0) : \bot..\bot\}$*, and* $T_2$ **nosel** $y_2$*, then* $\mathrm{F}_1;\rho \vdash T_2 <: \{\mathsf{M}(r_0) : \bot..\bot\}$.

*Proof.* By 5.99(ToSRed), exist $T_5$, $T_6$, such that $\mathrm{F}_2 \vdash T_2 \longmapsto^{\mathrm{s}}_{\oplus} T_5$, and $\mathrm{F}_2 \vdash \{\mathsf{M}(r_0) : \bot..\bot\} \longmapsto^{\mathrm{s}}_{\oplus} T_6$, and $\mathrm{F}_2;\rho \vdash^{\mathrm{s}}_{\oplus} T_5 <: T_6$. By 5.94(SRedMut), $T_6 = \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.92(SRedSub), $\mathrm{F}_2;\rho \vdash^{\mathrm{s}}_{\oplus} T_2 <: T_5$. By ($\mathrm{ST}^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F}_2;\rho \vdash^{\mathrm{s}}_{\oplus} T_2 <: \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.108(ToTRed), exist $T_7$, $T_8$, such that $T_2 \longmapsto^{\mathrm{m}}_{\oplus} T_7$, and $\{\mathsf{M}(r_0) : \bot..\bot\} \longmapsto^{\mathrm{m}}_{\oplus} T_8$, and $\mathrm{F}_2;\rho \vdash^{\mathrm{m}}_{\oplus} T_7 <: T_8$. By 5.100(TRedMut), $T_8 = \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.114(TRedCut), $\mathrm{F}_1;\rho \vdash T_2 <: T_7$, and $T_7$ **nosel** $y_2$, and $T_7 \longmapsto^{\mathrm{e}}_{\oplus} T_7$. By 5.115(TSubCut), exists $T_9$, such that $\{\mathsf{M}(r_0) : \bot..\bot\} \longmapsto^{\mathrm{e}}_{\oplus} T_9$, and $\mathrm{F}_1;\rho \vdash T_7 <: T_9$. By 5.101(ERedMut), $T_9 = \{\mathsf{M}(r_0) : \bot..\bot\}$. By (ST-Trans), $\mathrm{F}_1;\rho \vdash T_2 <: \{\mathsf{M}(r_0) : \bot..\bot\}$. □

**Lemma 5.122** (StnMFLoc). *If* $y_1 \neq y_2$*, and* $\mathrm{F}_2 = \mathrm{F}_1, y_2 : T$*, and* $\mathrm{F}_2;\rho \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$*, then* $\mathrm{F}_1;\rho \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$.

*Idea.* Adding a new location to the context cannot cause existing fields to become mutable. ▽

*Proof idea.* By typing equivalence in inert context and field typing inversion, $y_1$ has a field type, where the upper bound is a tight subtype of $\{\mathsf{M}(r_0) : \bot..\bot\}$. To show that this subtyping also holds without $y_2$ in the context, we take the subtyping derivation and remove unnecessary ($\mathrm{ST}_{\#}$-SelL) and ($\mathrm{ST}_{\#}$-SelU) applications, so that if we take the subtyping from left to right, type selection is only eliminated, not introduced. An exception to that is in applications of ($\mathrm{ST}_{\#}$-Met) rule. Next, we eliminate method types by replacing them by $\top$ in covariant positions and by $\bot$ in contravariant positions. Now the subtyping derivation never uses variables which are in $\mathrm{F}_2$ after $y_1$, and does not depend on subtyping in a different context. Therefore, the same derivation works in $\mathrm{F}_1$. ▽

*Proof.* By 5.77(VTEq), $\mathrm{F}_2;\rho \vdash_{\#\#} y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By 5.60(InvT), exist $T_3$, $T_4$, such that $\mathrm{F}_2 \vdash_{!} y_1 : \{a : T_3..T_4\}$, and $\mathrm{F}_2;\rho \vdash_{\#} T_4 <: \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.110(PrecCut), $\mathrm{F}_1 \vdash_{!} y_1 : \{a : T_3..T_4\}$. By 5.111(PrecFV), $y_2 \notin \mathrm{fv}\ T_4$. By 5.112(NoselFV), $T_4$ **nosel** $y_2$. By 5.121(StnSub), $\mathrm{F}_1;\rho \vdash T_4 <: \{\mathsf{M}(r_0) : \bot..\bot\}$. By (ST-Fld), $\mathrm{F}_1;\rho \vdash \{a : T_3..T_4\} <: \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By 5.78(VTEqB), $\mathrm{F}_1;\rho \vdash y_1 : \{a : T_3..T_4\}$. By (VT-Sub), $\mathrm{F}_1;\rho \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. □

### 5.2.9 Mutation lemmata

This section contains lemmata about mutable objects and mutability.

**Lemma 5.123** (ObjW). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, and* $y \to d \in \Sigma_1$*, then either* $y \to d \in \Sigma_2$ *or* $t_1 = w.a := x$*, and* $w \to y \in \rho_1$*.*

*Idea.* If a reduction step modifies an object, then it was a reduction of a write term referring to that object. ▽

*Proof.* By cases on typed reduction:

- Cases (TR-Read), (TR-Apply), (TR-LetLoc), (TR-LetPush): heap is not changed ($\Sigma_1 = \Sigma_2$), therefore $y \to d \in \Sigma_2$.
- Case (TR-LetNew): existing objects are not changed ($\Sigma_2 = \Sigma_1, y_2 \to d_2$), therefore $y \to d \in \Sigma_2$.
- Case (TR-Write): $t_1 = w.a := x$, and $\Sigma_2 = \Sigma_1[y_1 \to d_1]$, where $w \to y_1 \in \rho_1$. If $y_1 = y$, then $w \to y \in \rho_1$. Otherwise, the object is not changed, therefore $y \to d \in \Sigma_2$.

□

**Lemma 5.124** (MTS). *If* $\Gamma;\rho \vdash T_2 <: \bot$*, then* $\Gamma;\rho \vdash \{\mathsf{M}(r_0) : T_1..T_2\} <: \{\mathsf{M}(r_0) : \bot..\bot\}$*.*

*Proof.* By (ST-Bot), $\Gamma;\rho \vdash \bot <: T_1$. By (ST-Typ), $\Gamma;\rho \vdash \{\mathsf{M}(r_0) : T_1..T_2\} <: \{\mathsf{M}(r_0) : \bot..\bot\}$. □

**Lemma 5.125** (MMR). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, and* $y \to d \in \Sigma_1$*, then either* $y \to d \in \Sigma_2$ *or* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$*.*

*Idea.* If an object is mutated in a reduction step, then it must have been mutably reachable. ▽

*Proof idea.* Only reduction of write statements can modify objects. The reduction rule for write statements requires the target to be mutably reachable. ▽

*Proof.* By 5.123(ObjW), $t_1 = w.a := x$, and $w \to y \in \rho$. By (TF-Write1), $t_1$ $\mathbf{tfree}$ $w$. By inversion of (TR-Write), $\mathrm{F};\rho \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (Rea-Term), $\mathrm{F} \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$. □

**Lemma 5.126** (MPres). *If* $\mathrm{F} \vdash \langle t_2; \sigma_2; \rho; \Sigma\rangle$ $\mathbf{mreach}$ $y$*, and* $\forall x\colon (t_2 \ \mathbf{tfree}\ x \lor \sigma_2 \ \mathbf{tfree}\ x) \Rightarrow (t_1 \ \mathbf{tfree}\ x \lor \sigma_1 \ \mathbf{tfree}\ x)$*, then* $\mathrm{F} \vdash \langle t_1; \sigma_1; \rho; \Sigma\rangle$ $\mathbf{mreach}$ $y$*.*

*Idea.* If the heap and environment do not change, and the term and stack contain the same variables, then mutable reachability is preserved. ▽

*Proof idea.* Straightforward induction on mutable reachability. ▽

*Proof.* Induction on $\mathrm{F} \vdash \langle t_2; \sigma_2; \rho; \Sigma\rangle$ $\mathbf{mreach}$ $y$:

- Case (Rea-Fld): $\mathrm{F} \vdash \langle t_2; \sigma_2; \rho; \Sigma\rangle$ $\mathbf{mreach}$ $y_1$, and $y_1 \to \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma$, and $\mathrm{F};\rho \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By induction, $\mathrm{F} \vdash \langle t_1; \sigma_1; \rho; \Sigma\rangle$ $\mathbf{mreach}$ $y_1$ and (Rea-Fld).
- Case (Rea-Term): $w \to y \in \rho$, and $\mathrm{F};\rho \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. $(t_2 \ \mathbf{tfree}\ x \lor \sigma_2 \ \mathbf{tfree}\ x)$, therefore $(t_1 \ \mathbf{tfree}\ x \lor \sigma_1 \ \mathbf{tfree}\ x)$. By (Rea-Term).

□

## 5.3 Reduction lemmata

This section contains lemmata about the typed reduction relation defined in Section 4.1.

The progress lemmata, for each reduction rule, show that if the term of a configuration has a particular form, then the reduction rule can be applied. That may include proving that an involved object on the heap has a requested member. But note that because the typed reduction rules also involve types, the progress lemmata must reason about types too.

The progress lemmata are 5.135(PgRead), 5.142(PgWrite), 5.147(PgApply), 5.153(PgLetNew), 5.160(PgLetPush), and 5.165(PgLetLoc).

Type preservation lemmata, for each reduction rule, show that reduction preserves the type of the configuration. Because some of the reasoning about types is already part of the progress lemmata, the preservation lemmata can be a bit simpler than if they were defined for untyped reduction.

In each lemma, it has to be shown that the typing context remains inert, that the runtime environment and the heap correspond to the context, that the term has the type of the top of the stack, and that the type of the bottom of the stack does not change.

The type preservation lemmata are 5.136(TPRead), 5.143(TPWrite), 5.148(TPApply), 5.156(TPLetNew), 5.161(TPLetPush), and 5.166(TPLetLoc).

The **mreach** preservation lemmata, for each reduction rule, show that reduction does not make mutably reachable any existing object which is not mutably reachable.

The **mreach** preservation lemmata are mreach5.141(MPRead), 5.144(MPWrite), 5.150(MPApply), 5.159(MPLetNew), 5.163(MPLetPush), and 5.168(MPLetLoc).

### 5.3.1 Helper lemmata for progress and preservation

**Lemma 5.127** (HeapDP). *If* $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$, *and* $\mathrm{F};\rho_1 \vdash \mathrm{F}_0 \sim \Sigma_1$, *then there exists* $d$, *such that* $\mathrm{F}_0, y_1/s : R;\rho_1 \vdash d : [y_1/s]R$, *and* $y_1 \to d \in \Sigma_1$.

*Proof.* Induction on heap correspondence:

- Case (CT-EmptyH): not possible.
- Case (CT-ObjH): $\mathrm{F} = \mathrm{F}_3, y_0 : \mu(s_0 : R_0) \wedge \{\mathsf{M}(r_0) : \bot..T_0\}$, and $\Sigma_1 = \Sigma_3, y_0 \to d_0$, and $\mathrm{F}_3;\rho_1 \vdash \mathrm{F}_0 \sim \Sigma_3$, and $\mathrm{F}_0, y_0/s_0 : R_0;\rho_1 \vdash d_0 : [y_0/s_0]R_0$. If $y_0 = y_1$, then $d_0 = d$, and $s_0 = s$, and $R_0 = R$, therefore $\mathrm{F}_0, y_1/s : R;\rho_1 \vdash d : [y_1/s]R$, and $y_1 \to d \in \Sigma_1$. Otherwise by induction.
- Case (CT-RefH): $\mathrm{F} = \mathrm{F}_3, w : T$, and $\mathrm{F}_3;\rho_1 \vdash \mathrm{F}_0 \sim \Sigma_1$. By induction.

□

**Lemma 5.128** (HeapD). *If* $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$, *and* $\mathrm{F};\rho_1 \sim \Sigma_1$, *then there exists* $d$, *such that* $\mathrm{F}, y_1/s : R;\rho_1 \vdash d : [y_1/s]R$, *and* $y_1 \to d \in \Sigma_1$.

*Proof.* By inversion of (CT-CorrH), $\mathrm{F};\rho_1 \vdash \mathrm{F} \sim \Sigma_1$. By 5.127(HeapDP). □

**Lemma 5.129** (DSub). *If* $R = \ldots_3 R_1 \ldots_4$, *and* $\mathrm{F}, y/s : R;\rho \vdash d : R$, *then there exists* $d_1$, *such that* $d = \ldots_1 d_1 \ldots_2$, *and* $\mathrm{F}, y/s : R;\rho \vdash d_1 : R_1$.

*Proof.* Induction on $\mathrm{F}, y/s : R;\rho \vdash d : R$:

- Cases (HT-Typ), (HT-TypB), (HT-Fld), (HT-Met): $R = R_1$. Choose $d = d_1$.
- Case (HT-And): $d = d_2 \wedge d_3$. $R = R_2 \wedge R_3$. $\mathrm{F}, y/s : R;\rho \vdash d_2 : R_2$. $\mathrm{F}, y/s : R;\rho \vdash d_3 : R_3$. If $R_2 = \ldots_3 R_1 \ldots_5$, then by induction, $d_2 = \ldots_1 d_1 \ldots_6$. Otherwise, $R_3 = \ldots_5 R_1 \ldots_4$, then by induction, $d_3 = \ldots_6 d_1 \ldots_2$.

□

**Lemma 5.130** (DSubB). *If* $d = \ldots_1 d_1 \ldots_2$, *and* $\mathrm{F}, s : R;\rho \vdash d : R$, *then there exists* $R_1$, *such that* $R = \ldots_3 R_1 \ldots_4$, *and* $\mathrm{F}, s : R;\rho \vdash d_1 : R_1$.

*Proof.* Induction on $\mathrm{F}, s : R;\rho \vdash d : R$:

- Cases (DT-Typ), (DT-TypB), (DT-Fld), (DT-Met): $R = R_1$. Choose $d = d_1$.
- Case (DT-And): $d = d_2 \wedge d_3$. $R = R_2 \wedge R_3$. $\mathrm{F}, s : R;\rho \vdash d_2 : R_2$. $\mathrm{F}, s : R;\rho \vdash d_3 : R_3$. If $d_2 = \ldots_1 d_1 \ldots_6$, then by induction, $R_2 = \ldots_3 R_1 \ldots_5$. Otherwise, $d_3 = \ldots_6 d_1 \ldots_2$, then by induction, $R_3 = \ldots_5 R_1 \ldots_4$.

□

### 5.3.2 Read lemmata

In the (TR-Read) case, progress depends on existence of the field in the object on the heap, which is shown by 5.131(HeapF). The result type involves splitting the type of the field and adding the mutability of the receiver.

**Lemma 5.131** (HeapF). *If* $R = \ldots_3 \{a : T_5..T_5\} \ldots_4$, *and* $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$, *and* $\mathrm{F};\rho_1 \sim \Sigma_1$, *then there exists* $y_2$, *such that* $y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1$, *and* $\mathrm{F};\rho \vdash y_2 : [y_1/s]T_5$.

*Idea.* If an inert context gives a certain type to a field of an object, then in the corresponding heap, the object exists and the value of the field has that type. ▽

*Proof.* By 5.128(HeapD), there exists $d$, such that $\mathrm{F}, y_1/s : R;\rho \vdash d : [y_1/s]R$, and $y_1 \rightarrow d \in \Sigma_1$. By 5.129(DSub), there exists $d_1$, such that $d = \ldots_1 d_1 \ldots_2$, and $\mathrm{F}, y_1/s : R;\rho \vdash d_1 : [y_1/s]\{a : T_5..T_5\}$. By inversion of (HT-Fld), $d_1 = \{a = x\}$, and $\mathrm{F};\rho \vdash x : [y_1/s]T_5$. Because heap correspondence requires fields to be locations, then we can choose $y_2 = x$. □

**Lemma 5.132** (MuInv). *If* $\mathrm{F}_2;\rho_2 \vdash w_2 : \{\mathsf{M}(r_0) : \bot..\bot\}$, *where* $\mathrm{F}_2 = \mathrm{F}, w_2 : \mu(s_2 : R_2) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\}$, *then* $\mathrm{F}_2;\rho_2 \vdash_{\#} T_{13} <: \bot$.

*Idea.* If a reference is mutable, then its mutability in the context is $\bot$. ▽

*Proof.* By 5.77(VTEq), $\mathrm{F}_2;\rho_2 \vdash_{\#\#} w_2 : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (VT$_!$-Var) and (VT$_!$-And2), $\mathrm{F}_2 \vdash_! w_2 : \{\mathsf{M}(r_0) : \bot..T_{13}\}$. By 5.60(InvT), exists $T_{14}$, such that $\mathrm{F}_2 \vdash_! w_2 : \{\mathsf{M}(r_0) : \bot..T_{14}\}$, and $\rho_2;\rho \vdash_{\#} T_{14} <: \mathrm{F}_2$. By 5.52(UPrecTyp), $\rho_2 \vdash T_{14} \approx T_{13}$, therefore $\mathrm{F}_2;\rho_2 \vdash_{\#} T_{13} <: \bot$. □

**Lemma 5.133** (MAdapt). *If* $\mathrm{F}_2;\rho_2 \vdash w_2 : \{\mathsf{M}(r_0) : \bot..\bot\}$, *where* $\mathrm{F}_2 = \mathrm{F}, w_2 : \mu(s_2 : R_2) \wedge \{\mathsf{M}(r_0) : \bot..(T_7 \vee T_{13})\}$, *then* $\mathrm{F}_2;\rho_2 \vdash_{\#} T_7 <: \bot$, *and* $\mathrm{F}_2;\rho_2 \vdash_{\#} T_{13} <: \bot$.

*Proof.* By 5.132(MuInv), $\mathrm{F}_2;\rho_2 \vdash_{\#} T_7 \vee T_{13} <: \bot$. By (ST$_{\#}$-Or1) and (ST$_{\#}$-Or2) and (ST$_{\#}$-Trans), $\mathrm{F}_2;\rho_2 \vdash_{\#} T_7 <: \bot$, and $\mathrm{F}_2;\rho_2 \vdash_{\#} T_{13} <: \bot$. □

**Lemma 5.134** (RoVar). *If* $\mathrm{F};\rho_1 \vdash y_2 : T_3$, *where* $\mathrm{F} = \mathrm{F}_3, y_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_4$, *and* $\mathrm{F};\rho_1 \vdash T_3\ \mathbf{ro}\ T_6$, *then* $\mathrm{F}, w_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\};\rho_1, w_2 \rightarrow y_2 \vdash w_2 : T_6$.

*Proof.* $\mathrm{F}, w_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\}$ is an inert context, because the added type is based on a type in the context, and $w_2$ is not used in $\mathrm{F}$. By (CT-RefE), $\mathrm{F}, w_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\} \sim \rho_2$. By 5.5(Wkn), $\mathrm{F}, w_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\};\rho_1 \vdash y_2 : T_3$. By 5.7(WknE), $\mathrm{F}, w_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\};\rho_2 \vdash y_2 : T_3$. By 5.87(RefT), $\mathrm{F}, w_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..T_{13}\};\rho_2 \vdash w_2 : T_6$. □

**Lemma 5.135** (PgRead). *If* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$, *then there exists* $w_2$, *such that* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$.

*Proof idea.* By configuration and term typing inversion, 5.68(DerefT), typing equivalence, invertible typing inversion, inversion of precise typing and heap correspondence and 5.131(HeapF). ▽

*Proof.* By inversion of configuration typing, $\mathrm{F};\rho_1 \vdash w_1.a : T_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of (TT-Read), $\mathrm{F};\rho_1 \vdash w_1 : \{a : T_4..T_3\}$. By 5.68(DerefT), $\mathrm{F};\rho_1 \vdash y_1 : \{a : T_4..T_3\}$. By 5.77(VTEq), $\mathrm{F};\rho_1 \vdash_{\#\#} y_1 : \{a : T_4..T_3\}$. By 5.61(InvF), exist $T_9, T_8$, such that $\mathrm{F} \vdash_! y_1 : \{a : T_9..T_8\}$, and $\mathrm{F};\rho \vdash T_8 <: T_3$, and $\mathrm{F};\rho \vdash T_4 <: T_9$. By 5.58(CtxF), exists $T_5$, such that $\mathrm{F} = \mathrm{F}_1, y_1 : T, \mathrm{F}_2$, where $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $R = \ldots_3 \{a : T_5..T_5\} \ldots_4$, and $T_8 = [y_1/s]T_5$, and $T_9 = [y_1/s]T_5$. By 5.131(HeapF), $y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1$, and $\mathrm{F};\rho_1 \vdash y_2 : [y_1/s]T_5$. Choose fresh $w_2$. □

**Lemma 5.136** (TPRead). *If* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$, *then* $\mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle : T_0$.

*Proof idea.* Heap, stack and does not change, typing is preserved by weakening. The type of the new reference is a subtype of the term type and supertype of the location type. ▽

*Proof.* By inversion of typed reduction, $\mathrm{F};\rho_1 \vdash w_1.a : T_1$, and $\mathrm{F};\rho_1 \vdash y_2 : [y_1/s]T_5$, where $T_2 = \mu(s_1 : R_1) \wedge \{\mathsf{M}(r) : \bot..(T_7 \vee w_1.\mathsf{M}(r))\}$, and $\mathrm{F} = \mathrm{F}_3, y_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_4$. By inversion of (CT-Corr), $\mathrm{F};\rho_1 \sim \Sigma_1$, and $\mathrm{F} \sim \rho_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$.

- Inertness: Because $R_1$ comes from an inert context, $T_2$ is an inert type, and $w_2 \notin \mathrm{F}$, so $\mathrm{F}, w_2 : T_2$ is inert.

- Environment: By (CT-RefE), $\mathrm{F}, w_2 : T_2 \sim \rho_2$.
- Heap: By 5.12(WknH), $\mathrm{F}, w_2 : T_2;\rho_2 \sim \Sigma_1$.
- Term: By (TT-Sub), $\mathrm{F};\rho \vdash y_2 : T_3$. By 5.134(RoVar), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_2 : T_6$. By (VT-Var), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_2 : \mu(s_1 : R_1) \wedge \{\mathsf{M}(r) : \bot..(T_7 \vee w_1.\mathsf{M}(r))\}$. By (ST-And2) and (VT-Sub), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_2 : \{\mathsf{M}(r) : \bot..(T_7 \vee w_1.\mathsf{M}(r))\}$. By (VT-AndI), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_2 : T_1$. By (TT-Var), $\mathrm{F};\rho_2 \vdash \mathsf{v}w_2 : T_1$.
- Stack: By 5.6(WknS) and 5.9(EWknS), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash \sigma_1 : T_1, T_0$.

By (CT-Corr), $\mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle : T_0$. □

For preservation of **mreach**, we must show that if the resulting reference is mutable, then both the reference read from and the field read must have been mutable.

**Lemma 5.137** (WMu)**.** *If* $w_1 \neq w_2$, *and* $\mathrm{F}, w_2 : T_2;\rho_2 \vdash_{\#} w_1.\mathsf{M}(r) <: \bot$, *and* $\rho_2 = \rho_1, w_2 \to y_2$, *and* $\mathrm{F}, w_2 : T_2 \sim \rho_2$, *then* $\mathrm{F};\rho_1 \vdash w_1 : \{\mathsf{M}(r_2) : \bot..\bot\}$.

*Idea.* If a read resulted in a mutable reference, then the source reference was mutable. ▽

*Proof.* By (VT-MutTop), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_1 : \{\mathsf{M}(r_0) : \bot..\top\}$. By 5.60(InvT), exist $T_{20}$, $T_{21}$, such that $\mathrm{F}, w_2 : T_2 \vdash_{!} w_1 : \{\mathsf{M}(r_2) : T_{20}..T_{21}\}$. By (TR$^{\mathrm{s}}$-SelU), $\mathrm{F}, w_2 : T_2 \vdash w_1.\mathsf{M}(r) \longmapsto^{\mathrm{s}}_{\oplus} [r/r_2]T_{21}$. By (TR$^{\mathrm{s}}$-Refl), $\mathrm{F}, w_2 : T_2 \vdash \bot \longmapsto^{\mathrm{s}}_{\oplus} \bot$. By 5.98(SRedSubCom), exist $T_{22}$, $T_{23}$, such that $\mathrm{F}, w_2 : T_2 \vdash [r/r_2]T_{21} \longmapsto^{\mathrm{s}}_{\oplus} T_{22}$, and $\mathrm{F}, w_2 : T_2 \vdash \bot \longmapsto^{\mathrm{s}}_{\oplus} T_{23}$, and $\mathrm{F}, w_2 : T_2;\rho_2 \vdash^{\mathrm{s}}_{\oplus} T_{22} <: T_{23}$. By inversion of (TR$^{\mathrm{s}}$-Refl), $T_{23} = \bot$. By 5.92(SRedSub), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash^{\mathrm{s}}_{\oplus} [r/r_2]T_{21} <: T_{22}$. By (ST$^{\mathrm{s}}_{\#}$-Trans), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash^{\mathrm{s}}_{\oplus} [r/r_2]T_{21} <: T_{23}$. By 5.116(FromSSub), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash [r/r_2]T_{21} <: \bot$. By 5.33(SubR) and (TX-Bot), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash T_{21} <: \bot$. By 5.78(VTEqB), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_1 : \{\mathsf{M}(r_2) : T_{20}..T_{21}\}$. By (ST-Bot) and (ST-Typ) and (VT-Sub), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_1 : \{\mathsf{M}(r_2) : \bot..\bot\}$. By 5.117(StnMRef), $\mathrm{F};\rho_1 \vdash w_1 : \{\mathsf{M}(r_2) : \bot..\bot\}$. □

**Lemma 5.138** (MPReadObj)**.** *If* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$, *and* $\mathrm{F}, w_2 : T_2;\rho_2 \vdash_{\#} w_1.\mathsf{M}(r) <: \bot$, *and* $\rho_2 = \rho_1, w_2 \to y_2$, *and* $\mathrm{F}, w_2 : T_2 \sim \rho_2$, *and* $w_1 \to y_1 \in \rho_1$, *then* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y_1$.

*Idea.* If a read resulted in a mutable reference, then the source reference was mutable. ▽

*Proof.* By 5.137(WMu), $\mathrm{F};\rho_1 \vdash w_1 : \{\mathsf{M}(r_2) : \bot..\bot\}$. By (Rea-Term), $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y_1$. □

**Lemma 5.139** (MPReadFld)**.** *If* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$, *and* $\mathrm{F}, w_2 : T_2;\rho_2 \vdash_{\#} T_7 <: \bot$, *and* $w_1 \to y_1 \in \rho_1$, *and* $\mathrm{F};\rho_1 \vdash w_1 : \{a : T_4..T_3\}$, *and* $\mathrm{F};\rho_1 \vdash T_3$ **mu**$(r)$ $T_7$, *and* $\mathrm{F}, w_2 : T_2 \sim \rho_2$, *then* $\mathrm{F};\rho_1 \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$.

*Idea.* If a read resulted in a mutable reference, then the field was mutable. ▽

*Proof idea.* $T_7$ is an upper bound of the mutability of the field, therefore the field is mutable. Then we show that it also means it was mutable seen from a location in the original context and environment. ▽

*Proof.* By 5.35(MUSub), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash T_3 <: \{\mathsf{M}(r) : \bot..T_7\}$. By 5.78(VTEqB), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash T_7 <: \bot$. By (ST-Refl) and (ST-Typ), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash T_3 <: \{\mathsf{M}(r) : \bot..\bot\}$. By (ST-Fld) and (VT-Sub), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_1 : \{a : \bot..\{\mathsf{M}(r) : \bot..\bot\}\}$. By 5.120(StnMFRef), $\mathrm{F};\rho_1 \vdash w_1 : \{a : \bot..\{\mathsf{M}(r) : \bot..\bot\}\}$. By 5.68(DerefT), $\mathrm{F};\rho_1 \vdash y_1 : \{a : \bot..\{\mathsf{M}(r) : \bot..\bot\}\}$. Using alpha equivalence, $\mathrm{F};\rho_1 \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. □

**Lemma 5.140** (MPReadVal)**.** *If* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$, *and* $\rho_2 = \rho_1, w_2 \to y_2$, *and* $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w_2 : \{\mathsf{M}(r_0) : \bot..\bot\}$, *then* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y_2$.

*Idea.* This is the case where we need to show that the object pointed to by the resulting reference was mutable before. ▽

*Proof idea.* We need to show that its location was stored in a mutable field of $y_1$ and that $w_1$ was mutable. ▽

*Proof.* By inversion of (TR-Read), $y_1 \to \dots_1 \{a = y_2\} \dots_2 \in \Sigma_1$, where $w_1 \to y_1 \in \rho_1$, and $\mathrm{F};\rho_1 \vdash w_1 : \{a : T_4..T_3\}$, and $\mathrm{F};\rho_1 \vdash T_3$ **mu**$(r)$ $T_7$, and $T_2 = \mu(s_1 : R_1) \wedge \{\mathsf{M}(r) : \bot..(T_7 \vee w_1.\mathsf{M}(r))\}$. By 5.136(TPRead), $\mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle : T_0$. By inversion of (CT-Corr), $\mathrm{F}, w_2 : T_2 \sim \rho_2$.

By 5.133(MAdapt), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash_{\#} T_7 <: \bot$, and $\mathrm{F}, w_2 : T_2;\rho_2 \vdash_{\#} w_1.\mathsf{M}(r) <: \bot$. By 5.138(MPReadObj), $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y_1$. By 5.139(MPReadFld), $\mathrm{F};\rho_1 \vdash y_1 : \{a : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By (Rea-Fld), $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y_2$. □

**Lemma 5.141** (MPRead). *If* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$, *and* $\mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$, *then* $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$.

*Proof idea.* Stack and heap did not change, so the only new paths are starting from $y_2$. The new paths start with $\mathrm{F};\rho_1 \vdash y_2 : T_1$. If $w_2$ makes $y_2$ mutably reachable, then it must be mutable in $\mathrm{F}$. That happens only if both $w_1$ and the field $a$ in it were mutable, so $y_2$ was already mutably reachable. ▽

*Proof.* Induction on $\mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$:

- Case (Rea-Fld): $\mathrm{F}, w_2 : T_2 \vdash \langle \mathsf{v}w_2; \sigma_1; \rho_2; \Sigma_1\rangle$ $\mathbf{mreach}$ $y_0$, $y_0 \to \ldots_1 \{a_0 = y\} \ldots_2 \in \Sigma_1$, $\mathrm{F}, w_2 : T_2;\rho_2 \vdash y_0 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By induction, $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y_0$. By 5.120(StnMFRef), $\mathrm{F}, w_2 : T_2;\rho_2 \vdash y_0 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By (Rea-Fld), $\mathrm{F} \vdash \langle w_1.a; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$.
- Case (Rea-Term): $\mathsf{v}w_2$ $\mathbf{tfree}$ $w \vee \sigma_1$ $\mathbf{tfree}$ $w$, $w \to y \in \rho_2$, $\mathrm{F}, w_2 : T_2;\rho_2 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$.
  - If $w \neq w_2$, then $\sigma_1$ $\mathbf{tfree}$ $w$. By 5.117(StnMRef), $\mathrm{F};\rho_1 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (Rea-Term).
  - Otherwise, $w = w_2$, therefore $y = y_2$. By 5.140(MPReadVal).

□

### 5.3.3 Write lemmata

In the (TR-Write) case, progress requires existence of the field on the heap. The variable written must have the correct type.

**Lemma 5.142** (PgWrite). *If* $\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0$*, then there exists* $\Sigma_2$*, such that* $\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle \mathsf{v}w_3; \sigma_1; \rho_1; \Sigma_2 \rangle$*.*

*Proof idea.* By configuration typing and term typing inversion, the reference has a type compatible with the field type. By dereference typing, the location also has the type. By equivalence of typing in inert context, by inversion of invertible typing, by inversion of precise typing and heap correspondence, the type is compatible with the heap type of the field. Choose the new heap as a copy of the old heap with the value of $y_1.a$ changed to $y_3$. ▽

*Proof.* By inversion of (TR-Write), $\mathrm{F};\rho_1 \vdash w_1.a := w_3 : T_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of (TT-Write), $\mathrm{F};\rho_1 \vdash w_1 : \{a : T_3..T_2\}$, and $\mathrm{F};\rho_1 \vdash w_3 : T_3$. By 5.68(DerefT), $\mathrm{F};\rho_1 \vdash y_1 : \{a : T_3..T_2\}$. By equivalence of typing in inert context 5.77(VTEq), $\mathrm{F};\rho_1 \vdash_{\#\#} y_1 : \{a : T_3..T_2\}$. By 5.61(InvF), exist $T_9$, $T_8$, such that $\mathrm{F} \vdash_! y_1 : \{a : T_9..T_8\}$, and $\mathrm{F};\rho \vdash T_8 <: T_2$, and $\mathrm{F};\rho \vdash T_3 <: T_9$. By inversion of precise typing and heap correspondence 5.58(CtxF), exists $T_4$, such that $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$, where $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $R = \ldots_3 \{a : T_4..T_4\} \ldots_4$, and $T_8 = [y_1/s]T_4$, and $T_9 = [y_1/s]T_4$. By 5.131(HeapF), $y_1 \to \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1$. Choose $\Sigma_2 = \Sigma_1[y_1 \to \ldots_1 \{a = y_3\} \ldots_2]$. □

**Lemma 5.143** (TPWrite). *If* $\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle \mathsf{v}w_3; \sigma_1; \rho_1; \Sigma_2 \rangle$*, then* $\mathrm{F} \vdash \langle \mathsf{v}w_3; \sigma_1; \rho_1; \Sigma_2 \rangle : T_0$*.*

*Proof idea.* Context, environment and stack are preserved. Heap correspondence is the same for objects other than $y_1$. For the object $y_1$, it is the same for members other than the field $a$. ▽

*Proof.* By inversion of (TR-Write), $\mathrm{F};\rho_1 \vdash w_3 : T_3$, and $\mathrm{F};\rho_1 \vdash T_3 <: [y_1/s]T_4$, and $\mathrm{F};\rho_1 \vdash [y_1/s]T_4 <: T_2$. By inversion of (CT-Corr), $\mathrm{F};\rho_1 \sim \Sigma_1$, and $\mathrm{F} \sim \rho_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$.

For $a$ in $y_1$, we need to show that $\mathrm{F}, s : R;\rho \vdash y_3 : T_4$. By 5.68(DerefT), $\mathrm{F};\rho \vdash y_3 : T_3$. Because $\mathrm{F};\rho_1 \vdash T_3 <: [y_1/s]T_4$, by (VT-Sub), $\mathrm{F};\rho \vdash y_3 : [y_1/s]T_4$.

For the term: Because $\mathrm{F};\rho_1 \vdash [y_1/s]T_4 <: T_2$, by (ST-Trans), $\mathrm{F};\rho \vdash T_3 <: T_2$. By (VT-Sub), $\mathrm{F};\rho \vdash w_3 : T_2$. By (TT-Var), $\mathrm{F};\rho \vdash \mathsf{v}w_3 : T_2$. □

**Lemma 5.144** (MPWrite). *If* $\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle \mathsf{v}w_3; \sigma_1; \rho_1; \Sigma_2 \rangle$*, and* $\mathrm{F} \vdash \langle \mathsf{v}w_3; \sigma_1; \rho_1; \Sigma_2 \rangle$ **mreach** $y$*, then* $\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle$ **mreach** $y$*.*

*Proof idea.* Stack and term do not contain any new variables. If a location is mutably reachable through a field, then either it was reachable previously through the same field, or it is the field that was written to. In that case, the field written must have a mutable type, so the new value written must have already been mutable, and it was in the term. ▽

*Proof.* By inversion of (TR-Write), $\Sigma_2 = \Sigma_1[y_1 \to \ldots_1 \{a = y_3\} \ldots_2]$, and $\mathrm{F};\rho_1 \vdash w_1 : \{a : T_3..T_2\}$. Induction on mreach:

- Case (Rea-Term): $\mathsf{v}w_3$ **tfree** $w \vee \sigma_1$ **tfree** $w$, $w \to y \in \rho_1$, $\mathrm{F};\rho_1 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. If $\mathsf{v}w_3$ **tfree** $w$, then by inversion of (TF-Var) and (TF-Write2), $w_1.a := w_3$ **tfree** $w$. Otherwise, $\sigma_1$ **tfree** $w$. By (Rea-Term).
- Case (Rea-Fld): $\mathrm{F} \vdash \langle \mathsf{v}w_3; \sigma_1; \rho_1; \Sigma_2 \rangle$ **mreach** $y_0$, $y_0 \to \ldots_1 \{a_0 = y\} \ldots_2 \in \Sigma_2$, $\mathrm{F};\rho_1 \vdash y_0 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$.
  - If $y \neq y_3$, where $w_3 \to y_3 \in \rho_1$, then $y_0 \neq y_1$, so $y_0 \to \ldots_1 \{a_0 = y\} \ldots_2 \in \Sigma_1$. By induction, $\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle$ **mreach** $y_0$. By (Rea-Fld).
  - If $y = y_3$, and $y_0 \neq y_1$. $y_0 \to \ldots_1 \{a_0 = y\} \ldots_2 \in \Sigma_1$. By induction, $\mathrm{F} \vdash \langle w_1.a := w_3; \sigma_1; \rho_1; \Sigma_1 \rangle$ **mreach** $y_0$. By (Rea-Fld).
  - Otherwise, $y = y_3$, and $y_0 = y_1$. $R_0 = R = \ldots_3 \{a : T_4..T_4\} \ldots_4$. By 5.61(InvF) and 5.52(UPrecTyp), $\mathrm{F};\rho_1 \vdash_{\#} [y_1/s]T_4 <: \{\mathsf{M}(r_0) : \bot..\bot\}$. By (ST-Trans), $\Gamma;\rho \vdash T_3 <: \{\mathsf{M}(r_0) : \bot..\bot\}$. By (VT-Sub), $\mathrm{F};\rho_1 \vdash w_3 : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (TF-Write2), we have $w_1.a := w_3$ **tfree** $w_3$. By (Rea-Term).

□

### 5.3.4 Apply lemmata

In the (TR-Apply) case, progress requires existence of the method on the heap. The receiver and the argument must have the expected types.

**mreach** is preserved, because thanks to variable visibility, the only references in the resulting term can be the argument and the receiver.

**Lemma 5.145** (HeapM). *If* $R = \ldots_3 \{m(z : T_9, r : T_{11}) : T_{10}\} \ldots_4$*, and* $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$*, and* $\mathrm{F};\rho_1 \sim \Sigma_1$*, then there exists* $t$*, such that* $y_1 \to \ldots_1 \{m(z, r) = t\} \ldots_2 \in \Sigma_1$*, and* $\mathrm{F}, !, z : T_6, r : [y_1/s]R \wedge [r/s]R \wedge T_8;\rho_1 \vdash t : T_7$*, where* $T_6 = [y_1/s]T_9$*,* $T_8 = [y_1/s]T_{11}$*,* $T_7 = [y_1/s]T_{10}$*, and* $r \notin \mathrm{fv}\ R$*.*

*Idea.* If the context gives a type with a method to a location, than that object has a method of that type in the heap. ▽

*Proof.* By 5.128(HeapD), there exists $d$, such that $\mathrm{F}, y_1/s : R;\rho \vdash d : [y_1/s]R$, and $y_1 \to d \in \Sigma_1$. By 5.129(DSub), there exists $d_1$, such that $d = \ldots_1 d_1 \ldots_2$, and $\mathrm{F}, y_1/s : R;\rho \vdash d_1 : [y_1/s]\{m(z : T_9, r : T_{11}) : T_{10}\}$. By inversion of (HT-Met), $d_1 = \{m(z, r) = t\}$, and $\mathrm{F}, !, z : T_6, r : [y_1/s]R \wedge [r/s]R \wedge T_8;\rho_1 \vdash t : T_7$, and $r \notin \mathrm{fv}\ R$. □

**Lemma 5.146** (SubApply). *If* $\mathrm{F}, !, z : T_6, r : [y_1/s]R \wedge [r/s]R \wedge T_8;\rho_1 \vdash t : T_7$*, and* $\mathrm{F};\rho_1 \vdash w_2 : T_3$*, and* $\mathrm{F};\rho_1 \vdash w_1 : [w_2/z]T_5$*, where* $\mathrm{F};\rho_1 \vdash T_3 <: T_6$*,* $\mathrm{F}, z : T_3;\rho_1 \vdash T_5 <: T_8$*,* $\mathrm{F}, z : T_3, r : T_5;\rho_1 \vdash T_7 <: T_4$*, and* $T_1 = [w_1/r][w_2/z]T_4$*, and* $R$ **indep** $s$*, and* $r \notin \mathrm{fv}\ R$*, and* $\mathrm{F} \sim \rho_1$*, and* $\mathrm{F};\rho_1 \vdash w_1 : [w_1/s]R$*, and* $w_1 \to y_1 \in \rho_1$*, then* $\mathrm{F};\rho_1 \vdash [w_1/r][w_2/z]t : T_1$*.*

*Proof.* First, we substitute the argument $w_2$ for the parameter $z$. By 5.14(Unhide), $\mathrm{F}, z : T_6, r : [y_1/s]R \wedge [r/s]R \wedge T_8;\rho_1 \vdash t : T_7$. By (VT-Sub), $\mathrm{F};\rho_1 \vdash w_2 : T_6$. Because $z \notin \mathrm{dom}\ \mathrm{F}$, then by 5.33(SubR), $\mathrm{F};\rho_1 \vdash w_2 : [w_2/z]T_6$. By 5.5(Wkn), $\mathrm{F}, r : [w_2/z][y_1/s]R \wedge [w_2/z][r/s]R \wedge [w_2/z]T_8;\rho_1 \vdash w_2 : [w_2/z]T_6$. By 5.28(SubT), $\mathrm{F}, r : [w_2/z][y_1/s]R \wedge [w_2/z][r/s]R \wedge [w_2/z]T_8;\rho_1 \vdash [w_2/z]t : [w_2/z]T_7$. Because $z \notin \mathrm{fv}\ R$, $\mathrm{F}, r : [y_1/s]R \wedge [r/s]R \wedge [w_2/z]T_8;\rho_1 \vdash [w_2/z]t : [w_2/z]T_7$.

Second, we substitute the receiver $w_1$ for the parameter $r$. Because $z \notin \mathrm{dom}\ \mathrm{F}$, then by 5.33(SubR), $\mathrm{F};\rho_1 \vdash w_2 : [w_2/z]T_3$. By 5.27(SubV), $\mathrm{F};\rho_1 \vdash [w_2/z]T_5 <: [w_2/z]T_8$. By (VT-Sub), $\mathrm{F};\rho_1 \vdash w_1 : [w_2/z]T_8$. Because $r \notin \mathrm{dom}\ \mathrm{F}$, then by 5.33(SubR), $\mathrm{F};\rho_1 \vdash w_1 : [w_1/r][w_2/z]T_8$.

By 5.67(IndepEq), $\rho_1 \vdash [w_1/s]R \approx [y_1/s]R$. By (ST-Eq) and (VT-Sub), $\mathrm{F};\rho_1 \vdash w_1 : [y_1/s]R$. Because $r \notin \mathrm{dom}\ \mathrm{F}$, then by 5.33(SubR), $\mathrm{F};\rho_1 \vdash w_1 : [w_1/r][y_1/s]R$.

Because $r \notin \mathrm{fv}\ R$, $[w_1/s]R = [w_1/s][w_1/r]R$. By 5.21(SubSwap) and (VX-VarE), $[w_1/s][w_1/r]R = [w_1/r][r/s]R$, therefore $\mathrm{F};\rho_1 \vdash w_1 : [w_1/r][r/s]R$.

By (VT-AndI), $\mathrm{F};\rho_1 \vdash w_1 : [w_1/r][y_1/s]R \wedge [w_1/r][r/s]R$. By (VT-AndI), $\mathrm{F};\rho_1 \vdash w_1 : [w_1/r][y_1/s]R \wedge [w_1/r][r/s]R \wedge [w_1/r][w_2/z]T_8$. By (TX-And), $\mathrm{F};\rho_1 \vdash w_1 : [w_1/r]([y_1/s]R \wedge [r/s]R \wedge [w_2/z]T_8)$. By 5.28(SubT), $\mathrm{F};\rho_1 \vdash [w_1/r][w_2/z]t : [w_1/r][w_2/z]T_7$.

Finally, we adjust the result type. By 5.27(SubV), $\mathrm{F}, r : [w_2/z]T_5;\rho_1 \vdash [w_2/z]T_7 <: [w_2/z]T_4$. Because $r \notin \mathrm{dom}\ \mathrm{F}$, then by 5.33(SubR), $\mathrm{F};\rho_1 \vdash w_1 : [w_1/r][w_2/z]T_5$. By 5.27(SubV), $\mathrm{F};\rho_1 \vdash [w_1/r][w_2/z]T_7 <: [w_1/r][w_2/z]T_4$. By (TT-Sub), $\mathrm{F};\rho_1 \vdash [w_1/r][w_2/z]t : T_1$. □

**Lemma 5.147** (PgApply). *If* $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$*, then there exists* $t_2$*, such that* $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle t_2; \sigma_1; \rho_1; \Sigma_1\rangle$*.*

*Proof.* By inversion of configuration typing $\mathrm{F};\rho_1 \vdash w_1.m\, w_2 : T_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of term typing (TT-Apply), $\mathrm{F};\rho_1 \vdash w_1 : \{m(z : T_3, r : T_5) : T_4\}$, and $\mathrm{F};\rho_1 \vdash w_2 : T_3$. By 5.68(DerefT), $\mathrm{F};\rho_1 \vdash y_1 : \{m(z : T_3, r : T_5) : T_4\}$. By equivalence of typing in inert context 5.77(VTEq), $\mathrm{F};\rho_1 \vdash_{\#\#} y_1 : \{m(z : T_3, r : T_5) : T_4\}$. By inversion of invertible typing 5.62(InvM), $\mathrm{F} \vdash_{!} y_1 : \{m(z : T_6, r : T_8) : T_7\}$, $\mathrm{F};\rho_1 \vdash T_3 <: T_6$, $\mathrm{F}, z : T_3;\rho_1 \vdash T_5 <: T_8$, $\mathrm{F}, z : T_3, r : T_5;\rho_1 \vdash T_7 <: T_4$. Choose $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.57(CtxM), $\mathrm{F} = \mathrm{F}_1, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, \mathrm{F}_2$. By 5.145(HeapM), $y_1 \to \ldots_1 \{m(z, r) = t\} \ldots_2 \in \Sigma_1$, and $\mathrm{F}, !, z : T_6, r : [y_1/s]R \wedge [r/s]R \wedge T_8;\rho_1 \vdash t : T_7$. □

**Lemma 5.148** (TPApply). *If* $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/r][w_2/z]t; \sigma_1; \rho_1; \Sigma_1\rangle$*, then* $\mathrm{F} \vdash \langle [w_1/r][w_2/z]t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$*.*

*Proof idea.* Context, environment, heap and stack do not change. The new term has the expected type thanks to term typing and heap correspondence. ▽

*Proof.* By inversion of (TR-Apply), $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$, and $\mathrm{F}, !, z : T_6, r : [y_1/s]R \wedge [r/s]R \wedge T_8;\rho_1 \vdash t : T_7$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of (CT-Corr), $\mathrm{F};\rho_1 \sim \Sigma_1$, $\mathrm{F} \sim \rho_1$. By 5.146(SubApply), $\mathrm{F};\rho_1 \vdash [w_1/r][w_2/z]t : T_1$. By (CT-Corr), $\mathrm{F} \vdash \langle [w_1/r][w_2/z]t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$. □

**Lemma 5.149** (TFApply). *If* $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0$*, and* $y_1 \to \ldots_1 \{m(z,r) = t\} \ldots_2 \in \Sigma_1$*, and* $[w_1/r][w_2/z]t$ $\mathbf{tfree}$ $w \vee \sigma_1$ $\mathbf{tfree}$ $w$*, then* $w_1.m\, w_2$ $\mathbf{tfree}$ $w \vee \sigma_1$ $\mathbf{tfree}$ $w$*.*

*Idea.* Reducing method application does not make any variables t-free. ▽

*Proof.* If $\sigma_1$ $\mathbf{tfree}$ $w$, then trivially. Otherwise, $[w_1/r][w_2/z]t$ $\mathbf{tfree}$ $w$. By 5.47(TFSub), $w = w_1 \vee [w_2/z]t$ $\mathbf{tfree}$ $w$. If $w = w_1$, then by (TF-Apply1), $w_1.m\, w_2$ $\mathbf{tfree}$ $w$. Otherwise, by 5.47(TFSub), $w = w_2 \vee t$ $\mathbf{tfree}$ $w$. If $w = w_2$, then by (TF-Apply2), $w_1.m\, w_2$ $\mathbf{tfree}$ $w$. Otherwise, $t$ $\mathbf{tfree}$ $w$. Not possible by 5.46(MLoc). □

**Lemma 5.150** (MPApply). *If* $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1 \rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/r][w_2/z]t; \sigma_1; \rho_1; \Sigma_1 \rangle$*, and* $\mathrm{F} \vdash \langle [w_1/r][w_2/z]t; \sigma_1; \rho_1; \Sigma_1 \rangle$ $\mathbf{mreach}$ $y$*, then* $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1 \rangle$ $\mathbf{mreach}$ $y$*.*

*Proof idea.* By 5.46(MLoc), $t$ does not contain any locations. Therefore all variables in the term or on stack were there also before. Heap and context didn't change. Therefore everything mreach had to be mreach before by the same path. ▽

*Proof.* For each $w_0$, we show that if $[w_1/r][w_2/z]t$ $\mathbf{tfree}$ $w_0 \vee \sigma_1$ $\mathbf{tfree}$ $w_0$, then by 5.167(TFLetLoc), $w_1.m\, w_2$ $\mathbf{tfree}$ $w_0 \vee \sigma_1$ $\mathbf{tfree}$ $w_0$. By 5.126(MPres), $\mathrm{F} \vdash \langle w_1.m\, w_2; \sigma_1; \rho_1; \Sigma_1 \rangle$ $\mathbf{mreach}$ $y$. □

### 5.3.5 LetNew lemmata

In the (TR-LetNew) case, we must show that the heap and the typing contex have the correct form. For **mreach** preservation, we show that mutable fields of the new object must have been initialized by mutable references appearing in the term.

**Lemma 5.151** (DefTypRecord)**.** *If* $\mathrm{F}, s : T;\rho \vdash d : T$*, then* $T$ *is a record type.*

*Proof idea.* By induction on definition typing. ▽

*Proof.* Induction on $\mathrm{F}, s : T;\rho \vdash d : T$:

- Case (DT-Typ): $T = \{A(r) : T_1..T_1\}$.
- Case (DT-TypB): $T = \{A(r) : \bot..T_1\}$.
- Case (DT-Fld): $T = \{a : T_1..T_1\}$.
- Case (DT-Met): $T = \{m(z : T_1, r : T_2) : T_3\}$.
- Case (DT-And): $T = T_1 \wedge T_2$, and $d_1$ and $d_2$ have distinct member names. By induction, $T_1$ and $T_2$ are record types. Within $d_1$ and $d_2$, member names are unique, so they are also unique across $d_1 \wedge d_2$ .

□

**Lemma 5.152** (SubLetNew)**.** *If* $\mathrm{F}, z : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash t : T_1$*, then* $\mathrm{F}, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash [y_1/z]t : T_1$.

*Proof.* By 5.5(Wkn), $\mathrm{F}, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}, z : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash t : T_1$. By (VT-Var) and 5.27(SubV), $\mathrm{F}, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash y_1 : [y_1/z]\mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.27(SubV), $\mathrm{F}, y_1 : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho \vdash [y_1/z]t : T_1$. □

**Lemma 5.153** (PgLetNew)**.** *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$*, then there exist* $y_1$*,* $T$*,* $\Sigma_2$*, such that* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$.

*Proof.* By inversion of configuration typing $\mathrm{F};\rho_1 \vdash \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t : T_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of term typing (TT-New), $\mathrm{F}, s : R;\rho_1 \vdash d : R$, and $\mathrm{F}, z : \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\};\rho_1 \vdash t : T_1$. Choose fresh $w_1$ and $y_1$. Choose $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. Choose $\Sigma_2 = \Sigma_1, y_1 \to [y_1/s][\rho_1]d$. □

**Lemma 5.154** (CorrNewLoc)**.** *If* $\mathrm{F};\rho_1 \sim \Sigma_1$*, and* $\mathrm{F}, s : R;\rho_1 \vdash d : R$*, and* $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$*, and* $\Sigma_2 = \Sigma_1, y_1 \to [y_1/s][\rho_1]d$*, then* $\mathrm{F}, y_1 : T;\rho_1 \sim \Sigma_2$.

*Idea.* Adding a typed object to the heap and context preserves heap correspondence. ▽

*Proof idea.* Old objects are not changed and adding new variables to the context does not change their typing. The new object has the correct type thanks to term typing. ▽

*Proof.* By 5.69(DeD), $\mathrm{F}, s : R;\rho_1 \vdash [\rho_1]d : R$. By 5.5(Wkn), $\mathrm{F}, y_1 : T, s : R;\rho_1 \vdash [\rho_1]d : R$. By ($\mathrm{VT}_!$-Var) and ($\mathrm{VT}_!$-And1) and ($\mathrm{VT}_!$-Rec), $\mathrm{F}, y_1 : T \vdash_! y_1 : [y_1/s]R$. By 5.78(VTEqB), $\mathrm{F}, y_1 : T;\rho \vdash y_1 : [y_1/s]R$. By 5.29(SubD), $\mathrm{F}, y_1 : T, y_1/s : R;\rho_1 \vdash [y_1/s][\rho_1]d : [y_1/s]R$. By inversion of (CT-CorrH), $\mathrm{F};\rho_1 \vdash \mathrm{F} \sim \Sigma_1$. By 5.10(WknHL), $\mathrm{F}, y_1 : T;\rho_1 \vdash \mathrm{F} \sim \Sigma_1$. By (CT-ObjH), $\mathrm{F}, y_1 : T;\rho_1 \vdash \mathrm{F}, y_1 : T \sim \Sigma_2$. By (CT-CorrH), $\mathrm{F}, y_1 : T;\rho_1 \sim \Sigma_2$. □

**Lemma 5.155** (CorrNew)**.** *If* $\mathrm{F};\rho_1 \sim \Sigma_1$*, and* $\mathrm{F}, s : R;\rho_1 \vdash d : R$*, and* $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$*, and* $\Sigma_2 = \Sigma_1, y_1 \to [y_1/s][\rho_1]d$*, and* $\rho_2 = \rho_1, w_1 \to y_1$*, then* $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \sim \Sigma_2$.

*Idea.* Adding a typed object to the heap and context and a reference to the environment preserves heap correspondence. ▽

*Proof idea.* Old objects are not changed and adding new variables to the context does not change their typing. The new object has the correct type thanks to term typing. ▽

*Proof.* By 5.154(CorrNewLoc), $\mathrm{F}, y_1 : T;\rho_1 \sim \Sigma_2$. By 5.12(WknH), $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \sim \Sigma_2$. □

**Lemma 5.156** (TPLetNew)**.** *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$*, then* $\mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle : T_0$.

*Proof idea.* Objects on the heap except $y_1$ are typed the same. By typing of the term, the new object has the specified type. Context is extended, typing is preserved by weakening. ▽

*Proof.* By inversion of (TR-LetNew), $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$, and $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$. By inversion of (CT-Corr), $\mathrm{F};\rho_1 \sim \Sigma_1$, and $\mathrm{F} \sim \rho_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$.

- Inertness: By 5.151(DefTypRecord), $R$ is a record type, therefore $T$ is inert, and $y_1$ and $w_1$ are fresh, so $T$ does not refer to them, therefore $\mathrm{F}, y_1 : T, w_1 : T$ is inert.
- Environment correspondence: By (CT-RefE), $\mathrm{F}, y_1 : T, w_1 : T \sim \rho_2$.
- Heap correspondence: By 5.155(CorrNew), $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \sim \Sigma_2$.
- Term typing: By 5.152(SubLetNew), $\mathrm{F}, y_1 : T, w_1 : T;\rho \vdash [w_1/z]t : T_1$.
- Stack typing: By 5.6(WknS), $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash \sigma_1 : T_1, T_0$.

By (CT-Corr), $\mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle : T_0$. □

**Lemma 5.157** (MPLetNewVal). *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$*, and* $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash y_1 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$*, and* $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$*, and* $\mathrm{F}, s : R;\rho_1 \vdash d : R$*, and* $d = \ldots_7 \{a_0 = w\} \ldots_8$*, and* $\mathrm{F}, y_1 : T, w_1 : T \sim \rho_2$*, and* $\rho_2 = \rho_1, w_1 \to y_1$*, then* $\mathrm{F};\rho_1 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$.

*Proof.* By 5.77(VTEq), $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash_{\#\#} y_1 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By 5.61(InvF), $\mathrm{F}, y_1 : T, w_1 : T \vdash_! y_1 : \{a : T_{12}..T_{10}\}$, where $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash_\# T_{10} <: \{\mathsf{M}(r_0) : \bot..\bot\}$.

By 5.130(DSubB), $R = \ldots_3 R_1 \ldots_4$, such that $\mathrm{F}, s : R;\rho_1 \vdash \{a_0 = w\} : R_1$. By inversion of (DT-Fld), $R_1 = \{a : T_{11}..T_{11}\}$, and $\mathrm{F}, s : R;\rho_1 \vdash w : T_{11}$. By (VT-Var) and (ST-And1) and (VT-Sub) and (VT-RecE), $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash y_1 : [y_1/s]R$. By 5.5(Wkn) and 5.27(SubV), $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash w : [y_1/s]T_{11}$. By 5.58(CtxF), and because declarations in $R$ have unique names, $[y_1/s]T_{11} = T_{10}$, therefore $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash_\# [y_1/s]T_{11} <: \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.78(VTEqB) and (VT-Sub), $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. By 5.117(StnMRef) and 5.119(StnMLoc), $\mathrm{F};\rho_1 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. □

**Lemma 5.158** (MPLetNewFld). *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$*, and* $y_1 \to \ldots_1 \{a_0 = y\} \ldots_2 \in \Sigma_2$*, and* $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash y_1 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$*, and* $y \neq y_1$*, then* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$.

*Idea.* If an object with a mutable field was created, then its value was a mutable reference in the creation term. ▽

*Proof idea.* Because the new object has the field $a_0$ in the heap, then the definition of the object must contain definition of that field with some value $w$. This value is therefore t-free in the term. Because the field is mutable, the value must also be mutable. ▽

*Proof.* By inversion of (TR-LetNew), $\Sigma_2 = \Sigma_1, y_1 \to [y_1/s][\rho_1]d$, and $\mathrm{F}, s : R;\rho_1 \vdash d : R$, and $T = \mu(s : R) \wedge \{\mathsf{M}(r_0) : \bot..\bot\}$, and $\rho_2 = \rho_1, w_1 \to y_1$. By 5.156(TPLetNew), $\mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle : T_0$. By inversion of (CT-Corr), $\mathrm{F}, y_1 : T, w_1 : T \sim \rho_2$.

We know that $[y_1/s][\rho_1]d = \ldots_1 \{a_0 = y\} \ldots_2$. Because $y \neq y_1$, therefore $[\rho_1]d = \ldots_5 \{a_0 = y\} \ldots_6$. By 5.70(DeInv), there is $w$, such that $\{a_0 = w\} \in d$, and $w \to y \in \rho_1$. By (TF-Fld) and (TF-And1) or by (TF-And2), $d$ $\mathbf{tfree}$ $w$. By (TF-NewD), $\mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t$ $\mathbf{tfree}$ $w$.

By 5.157(MPLetNewVal), $\mathrm{F};\rho_1 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (Rea-Term), $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$. □

**Lemma 5.159** (MPLetNew). *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$*, and* $\mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$ $\mathbf{mreach}$ $y$*, then* $y \notin \mathrm{F}$ *or* $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$.

*Proof idea.* If something is mreach from $\sigma_1$, then it was mreach by the same path. If something is mreach from $[w_1/z]t$ starting from location other than $y_1$, then it was mreach by the same path from $t$. If something is mreach from $[w_1/z]t$ starting from $y_1$, then it is either $y_1$ itself, or the path continues through a field, and the value of the field was occurring in the term. If the field is mutable, then the value must have been a mutable reference. ▽

*Proof.* Induction on $\mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$ $\mathbf{mreach}$ $y$:

- Case (Rea-Fld): $\mathrm{F}, y_1 : T, w_1 : T \vdash \langle [w_1/z]t; \sigma_1; \rho_2; \Sigma_2\rangle$ **mreach** $y_0$, $y_0 \to \ldots_1 \{a_0 = y\} \ldots_2 \in \Sigma_2$, $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash y_0 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By induction, $\mathrm{F} \vdash \langle \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y_0$.
    - If $y_0 \neq y_1$, then $y_0 \to \ldots_1 \{a_0 = y\} \ldots_2 \in \Sigma_1$. By 5.122(StnMFLoc) and 5.120(StnMFRef), $\mathrm{F}; \rho_1 \vdash y_0 : \{a_0 : \bot..\{\mathsf{M}(r_0) : \bot..\bot\}\}$. By (Rea-Fld).
    - Otherwise, $y_0 = y_1$, then $\{a_0 = y\} \in [y_1/s][\rho_1]d$. If $y = y_1$, then $y \notin \mathrm{F}$. Otherwise, by 5.158(MPLetNewFld).
- Case (Rea-Term): $[w_1/z]t$ **tfree** $w \vee \sigma_1$ **tfree** $w$, $w \to y \in \rho_2$, $\mathrm{F}, y_1 : T, w_1 : T;\rho_2 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. If $[w_1/z]t$ **tfree** $w$, then $y = y_1$, so $y \notin \mathrm{F}$. Otherwise, $\sigma_1$ **tfree** $w$. By 5.119(StnMLoc) and 5.117(StnMRef), $\mathrm{F};\rho_1 \vdash w : \{\mathsf{M}(r_0) : \bot..\bot\}$. By (Rea-Term).

□

### 5.3.6 LetPush lemmata

The (TR-LetPush) and (TR-LetLoc) are simple cases only involving moving a term between the focus and the stack.

**Lemma 5.160** (PgLetPush). *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$*, then there exists* $\sigma_2$*, such that* $\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1\rangle$.

*Proof.* By inversion of configuration typing $\mathrm{F};\rho_1 \vdash \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2 : T_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of term typing (TT-Let), $\mathrm{F};\rho_1 \vdash t_1 : T_3$, and $\mathrm{F}, z : T_3;\rho_1 \vdash t_2 : T_1$. Choose $\sigma_2 = \mathsf{let}\ z = \square\ \mathsf{in}\ t_2 :: \sigma_1$. □

**Lemma 5.161** (TPLetPush). *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1\rangle$*, then* $\mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1\rangle : T_0$.

*Proof idea.* Context, environment and heap are the same. ▽

*Proof.* By inversion of (TR-LetPush), $\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0$, and $\mathrm{F};\rho_1 \vdash t_1 : T_3$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of (CT-Corr), $\mathrm{F};\rho_1 \sim \Sigma_1$, and $\mathrm{F} \sim \rho_1$. By (CT-LetS), $\mathrm{F};\rho \vdash \sigma_2 : T_3, T_0$. By (CT-Corr), $\mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1\rangle : T_0$. □

**Lemma 5.162** (TFLetPush). *If* $\sigma_2 = \mathsf{let}\ z = \square\ \mathsf{in}\ t_2 :: \sigma_1$*, and* $t_1$ $\mathbf{tfree}$ $w \lor \sigma_2$ $\mathbf{tfree}$ $w$*, then* $\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$ $\mathbf{tfree}$ $w \lor \sigma_1$ $\mathbf{tfree}$ $w$.

*Idea.* Reducing a let term does not make any variables t-free. ▽

*Proof.* If $t_1$ $\mathbf{tfree}$ $w$, then by (TF-LetPush), $\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$ $\mathbf{tfree}$ $w$. Otherwise, $\sigma_2$ $\mathbf{tfree}$ $w$. By inversion:

Case (TF-LetST): $t_2$ $\mathbf{tfree}$ $w$. By (TF-LetPop), $\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$ $\mathbf{tfree}$ $w$.

Case (TF-LetSS): $\sigma_1$ $\mathbf{tfree}$ $w$. □

**Lemma 5.163** (MPLetPush). *If* $\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1\rangle$*, and* $\mathrm{F} \vdash \langle t_1; \sigma_2; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$*, then* $\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$.

*Proof idea.* Locations could only move from term to stack. All variables in $t_1$ or $\sigma_2$ were also in $\sigma_1$ or $\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$. Heap and context didn't change. Therefore everything mreach had to be mreach before by the same path. ▽

*Proof.* For each $t_1$ $\mathbf{tfree}$ $w_0 \lor \sigma_2$ $\mathbf{tfree}$ $w_0$. By 5.167(TFLetLoc), $\mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$ $\mathbf{tfree}$ $w_0 \lor \sigma_1$ $\mathbf{tfree}$ $w_0$. By 5.126(MPres), $\mathrm{F} \vdash \langle \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2; \sigma_1; \rho_1; \Sigma_1\rangle$ $\mathbf{mreach}$ $y$. □

### 5.3.7 LetLoc lemmata

**Lemma 5.164** (SubLetLoc). *If* $\mathrm{F}, z : T_1;\rho \vdash t : T_3$*, and* $\mathrm{F};\rho \vdash w_1 : T_1$*, then* $\mathrm{F};\rho \vdash [w_1/z]t : T_3$.

*Proof.* By 5.27(SubV). □

**Lemma 5.165** (PgLetLoc). *If* $\mathrm{F} \vdash \langle \mathsf{v}w_1;\sigma_1;\rho_1;\Sigma_1\rangle : T_0$*, and* $\sigma_1 = \mathsf{let}\ z = \Box\ \mathsf{in}\ t :: \sigma_2$*, then there exists* $t_2$*, such that* $\mathrm{F} \vdash \langle \mathsf{v}w_1;\sigma_1;\rho_1;\Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle t_2;\sigma_2;\rho_1;\Sigma_1\rangle$.

*Proof.* By inversion of configuration typing, $\mathrm{F};\rho_1 \vdash \mathsf{v}w_1 : T_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. Choose $t_2 = [w_1/z]t$. □

**Lemma 5.166** (TPLetLoc). *If* $\mathrm{F} \vdash \langle \mathsf{v}w_1;\sigma_1;\rho_1;\Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/z]t;\sigma_2;\rho_1;\Sigma_1\rangle$*, then* $\mathrm{F} \vdash \langle [w_1/z]t;\sigma_2;\rho_1;\Sigma_1\rangle : T_0$.

*Proof idea.* Context, environment and heap are preserved. ▽

*Proof.* By inversion of (TR-LetLoc), $\mathrm{F} \vdash \langle \mathsf{v}w_1;\sigma_1;\rho_1;\Sigma_1\rangle : T_0$, and $\mathrm{F};\rho_1 \vdash \mathsf{v}w_1 : T_1$, and $\mathrm{F};\rho_1 \vdash \sigma_1 : T_1, T_0$. By inversion of (CT-Corr), $\mathrm{F};\rho_1 \sim \Sigma_1$, and $\mathrm{F} \sim \rho_1$. By inversion of (CT-LetS), there exists $T_3$, such that $\mathrm{F};\rho \vdash \sigma_2 : T_3, T_0$, and $\mathrm{F}, z : T_1;\rho \vdash t : T_3$. By inversion of (TT-Var), $\mathrm{F};\rho \vdash w_1 : T_3$. By 5.164(SubLetLoc), $\mathrm{F};\rho \vdash [w_1/z]t : T_3$. By (CT-Corr), $\mathrm{F} \vdash \langle [w_1/z]t;\sigma_2;\rho_1;\Sigma_1\rangle : T_0$. □

**Lemma 5.167** (TFLetLoc). *If* $\sigma_1 = \mathsf{let}\ z = \Box\ \mathsf{in}\ t :: \sigma_2$*, and* $[w_1/z]t\ \mathbf{tfree}\ w \vee \sigma_2\ \mathbf{tfree}\ w$*, then* $\mathsf{v}w_1\ \mathbf{tfree}\ w \vee \sigma_1\ \mathbf{tfree}\ w$.

*Idea.* Reducing the stack does not make any variables t-free. ▽

*Proof.* If $\sigma_2\ \mathbf{tfree}\ w$, then by (TF-LetSS), $\sigma_1\ \mathbf{tfree}\ w$. If $[w_1/z]t\ \mathbf{tfree}\ w$, then by 5.47(TFSub), $w = w_1 \vee w\ \mathbf{tfree}\ t$. If $w = w_1$, then by (TF-Var), $\mathsf{v}w_1\ \mathbf{tfree}\ w$. Otherwise, $t\ \mathbf{tfree}\ w$. By (TF-LetSS), $\sigma_1\ \mathbf{tfree}\ w$. □

**Lemma 5.168** (MPLetLoc). *If* $\mathrm{F} \vdash \langle \mathsf{v}w_1;\sigma_1;\rho_1;\Sigma_1\rangle : T_0 \longmapsto \mathrm{F} \vdash \langle [w_1/z]t;\sigma_2;\rho_1;\Sigma_1\rangle$*, and* $\mathrm{F} \vdash \langle [w_1/z]t;\sigma_2;\rho_1;\Sigma_1\rangle\ \mathbf{mreach}\ y$*, then* $\mathrm{F} \vdash \langle \mathsf{v}w_1;\sigma_1;\rho_1;\Sigma_1\rangle\ \mathbf{mreach}\ y$.

*Proof idea.* Locations could only move from the stack to the term. All variables in the term were in the term or on the stack before. Heap and context didn't change. Therefore everything mreach had to be mreach before by the same path. ▽

*Proof.* For each $[w_1/z]t\ \mathbf{tfree}\ w_0 \vee \sigma_2\ \mathbf{tfree}\ w_0$, we have by 5.167(TFLetLoc), $\mathsf{v}w_1\ \mathbf{tfree}\ w_0 \vee \sigma_1\ \mathbf{tfree}\ w_0$. By 5.126(MPres), $\mathrm{F} \vdash \langle \mathsf{v}w_1;\sigma_1;\rho_1;\Sigma_1\rangle\ \mathbf{mreach}\ y$. □

### 5.3.8 Reduction equivalence

Reduction rules are defined to be similar to kDOT [2] reduction rules. They do not use types of terms or variables in any way. In order to prove preservation, typed reduction is defined to be similar to reduction, but requires the configuration to be typed. This is most important for (TR-Read). Typed reduction is more complicated than reduction, so soundness theorems are stated for normal reduction. By showing equivalence between typed and normal reduction, soundness is proven for normal reduction.

**Lemma 5.169** (REq). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle : T \longmapsto \mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2 \rangle$*, then* $\langle t_1; \sigma_1; \rho; \Sigma_1 \rangle \longmapsto \langle t_2; \sigma_2; \rho; \Sigma_2 \rangle$.

*Proof idea.* Straightforward correspondence between cases of typed reduction and normal reduction. ▽

*Proof.* By cases on typed reduction:

- Case (TR-Read): $w_1 \rightarrow y_1 \in \rho_1$, and $y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1$, and $\rho_2 = \rho_1, w_2 \rightarrow y_2$, and $t_1 = w_1.a$, and $t_2 = \mathsf{v} w_2$, and $\sigma_1 = \sigma_2$, and $\Sigma_1 = \Sigma_2$. By (R-Read).
- Case (TR-Write): $w_1 \rightarrow y_1 \in \rho_1$, and $w_3 \rightarrow y_3 \in \rho_1$, and $y_1 \rightarrow \ldots_1 \{a = y_2\} \ldots_2 \in \Sigma_1$, and $\Sigma_2 = \Sigma_1[y_1 \rightarrow \ldots_1 \{a = y_3\} \ldots_2]$, and $t_1 = w_1.a := w_3$, and $t_2 = \mathsf{v} w_3$, and $\sigma_1 = \sigma_2$. By (R-Write).
- Case (TR-Apply): $w_1 \rightarrow y_1 \in \rho_1$, and $y_1 \rightarrow \ldots_1 \{m(z, r) = t\} \ldots_2 \in \Sigma_1$, and $t_1 = w_1.m\, w_2$, and $t_2 = [w_1/r][w_2/z]t$, and $\sigma_1 = \sigma_2$, and $\Sigma_1 = \Sigma_2$. By (R-Apply).
- Case (TR-LetNew): $\rho_2 = \rho_1, w_1 \rightarrow y_1$, and $\Sigma_2 = \Sigma_1, y_1 \rightarrow [y_1/s][\rho_1]d$, and $t_1 = \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t$, and $t_2 = [w_1/z]t$, and $\sigma_1 = \sigma_2$. By (R-LetNew).
- Case (TR-LetPush): $t_1 = \mathsf{let}\ z = t_2\ \mathsf{in}\ t_3$, and $\sigma_2 = \mathsf{let}\ z = \Box\ \mathsf{in}\ t_3 :: \sigma_1$, and $\Sigma_1 = \Sigma_2$. By (R-LetPush).
- Case (TR-LetLoc): $t_1 = \mathsf{v} w_1$, and $t_2 = [w_1/z]t$, and $\sigma_1 = \mathsf{let}\ z = \Box\ \mathsf{in}\ t :: \sigma_2$, and $\Sigma_1 = \Sigma_2$. By (R-LetLoc).

□

**Lemma 5.170** (RjEq). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle : T \longmapsto^j \mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2 \rangle$*, then* $\langle t_1; \sigma_1; \rho; \Sigma_1 \rangle \longmapsto^j \langle t_2; \sigma_2; \rho; \Sigma_2 \rangle$.

*Proof.* Induction on number of steps using 5.169(REq). □

## 5.4 Theorems

This section contains the main properties of the type system, notably the Type soundness Theorem 5.173(S) and the Immutability Gurantee 5.181(IG).

For soundness, Theorem 5.171(TPP) combines progress and preservation for a single step of typed reduction. When applied to an arbitrary number of steps, Theorem 5.172(TyS) is a type soundness theorem for typed reduction.

**Theorem 5.171** (TPP). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T$*, then either* $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle = \langle \mathsf{v}w_1; \cdot; \rho_1; \Sigma_1\rangle$*, or exists* $t_2$*,* $\sigma_2$*,* $\Sigma_2$*,* $\rho_2$*,* $\mathrm{F}_2$*, such that* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, and* $\mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle : T$*.*

*Proof.* By cases on $t_1$:

- If $t_1 = \mathsf{v}x_1$, then by 5.41(RFV), $t_1 = \mathsf{v}w_1$.
- If $t_1 = \mathsf{v}w_1$, and $\sigma_1 = \cdot$, then it is answer.
- If $t_1 = \mathsf{v}w_1$, and $\sigma_1 = \mathsf{let}\ z = \square\ \mathsf{in}\ t :: \sigma_2$, then by 5.165(PgLetLoc) and 5.166(TPLetLoc).
- If $t_1 = \mathsf{let}\ z = t_1\ \mathsf{in}\ t_2$, then by 5.160(PgLetPush) and 5.161(TPLetPush).
- If $t_1 = \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t$, then by 5.153(PgLetNew) and 5.156(TPLetNew).
- If $t_1 = x_1.m\, x_2$, then by 5.41(RFV), $t_1 = w_1.m\, w_2$. By 5.147(PgApply) and 5.148(TPApply).
- If $t_1 = x_1.a := x_3$, then by 5.41(RFV), $t_1 = w_1.a := w_3$. By 5.142(PgWrite) and 5.143(TPWrite).
- If $t_1 = x_1.a$, then by 5.41(RFV), $t_1 = w_1.a$. By 5.135(PgRead) and 5.136(TPRead).

□

**Theorem 5.172** (TyS). *If* $\vdash t_0 : T$*, then either* $\exists w, j, \Sigma, \rho, \mathrm{F}\colon \vdash \langle t_0; \cdot; \cdot; \cdot\rangle : T \longmapsto^j \mathrm{F} \vdash \langle \mathsf{v}w; \cdot; \rho; \Sigma\rangle$ *or* $\forall j\colon \exists t_j, \sigma_j, \Sigma_j, \rho_j, \mathrm{F}_j\colon \vdash \langle t_0; \cdot; \cdot; \cdot\rangle : T \longmapsto^j \mathrm{F}_j \vdash \langle t_j; \sigma_j; \rho_j; \Sigma_j\rangle$*.*

*Proof.* By configuration typing, $;\rho \vdash \langle t_0; \cdot; \cdot; \cdot\rangle : T$. For every $j \geq 0$, if $\langle t_j; \sigma_j; \rho_j; \Sigma_j\rangle$ is an answer, then first alternative holds. Otherwise, compute configuration $\langle t_{j+1}; \sigma_{j+1}; \rho_{j+1}; \Sigma_{j+1}\rangle$ using 5.171(TPP), and continue for $j + 1$. If no such $j$ produces an answer, then the second alternative holds. □

Theorem S is a type soundness theorem based on kDOT [2], stating that typed contexts reduce to an answer or diverge. Instead of using Progress and Preservation lemmata for untyped reduction, we use the type safety theorem for typed reduction, and ignore the types.

**Theorem 5.173** (S). *If* $\vdash t_0 : T$*, then either* $\exists y, j, \Sigma, \rho\colon \langle t_0; \cdot; \cdot; \cdot\rangle \longmapsto^j \langle \mathsf{v}y; \cdot; \rho; \Sigma\rangle$ *or* $\forall j\colon \exists t_j, \sigma_j, \Sigma_j, \rho_j\colon \langle t_0; \cdot; \cdot; \cdot\rangle \longmapsto^j \langle t_j; \sigma_j; \rho_j; \Sigma_j\rangle$*.*

*Proof.* By 5.172(TyS), either $\exists w, j, \Sigma, \rho, \mathrm{F}\colon \vdash \langle t_0; \cdot; \cdot; \cdot\rangle : T \longmapsto^j \mathrm{F} \vdash \langle \mathsf{v}w; \cdot; \rho; \Sigma\rangle$, or $\forall j\colon \exists t_j, \sigma_j, \Sigma_j, \rho_j, \mathrm{F}_j\colon \vdash \langle t_0; \cdot; \cdot; \cdot\rangle : T \longmapsto^j \mathrm{F}_j \vdash \langle t_j; \sigma_j; \rho_j; \Sigma_j\rangle$. By 5.170(RjEq), either $\exists y, j, \Sigma, \rho, \mathrm{F}\colon \vdash \langle t_0; \cdot; \cdot; \cdot\rangle : T \longmapsto^j \mathrm{F} \vdash \langle \mathsf{v}y; \cdot; \rho; \Sigma\rangle$, or $\forall j\colon \exists t_j, \sigma_j, \Sigma_j, \rho_j, \mathrm{F}_j\colon \vdash \langle t_0; \cdot; \cdot; \cdot\rangle : T \longmapsto^j \mathrm{F}_j \vdash \langle t_j; \sigma_j; \rho_j; \Sigma_j\rangle$. □

We can also state the traditional Progress and Preservation lemmata of untyped reduction.

**Lemma 5.174** (Pg). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T$*, then either* $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle = \langle \mathsf{v}w_1; \cdot; \rho_1; \Sigma_1\rangle$*, or exists* $t_2$*,* $\sigma_2$*,* $\Sigma_2$*,* $\rho_2$*,* $\mathrm{F}_2$*, such that* $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \longmapsto \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*.*

*Proof.* By 5.171(TPP), either $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle = \langle \mathsf{v}w_1; \cdot; \rho_1; \Sigma_1\rangle$, or exist $t_2$, $\sigma_2$, $\Sigma_2$, $\rho_2$, $\mathrm{F}_2$, such that $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$, and $\mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle : T$. By 5.169(REq), $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \longmapsto \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$. □

**Lemma 5.175** (TPEq). *If* $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \longmapsto \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, and* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T$*, then* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, and* $\mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle : T$*.*

*Proof.* By 5.171(TPP), either $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle = \langle \mathsf{v}w_1; \cdot; \rho_1; \Sigma_1\rangle$, or exist $t_3$, $\sigma_3$, $\Sigma_3$, $\rho_3$, $\mathrm{F}_3$, such that $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_1, \mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle$, and $\mathrm{F}_1, \mathrm{F}_3;\rho \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle : T$. Because $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \longmapsto \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$, therefore $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \neq \langle \mathsf{v}w_1; \cdot; \rho_1; \Sigma_1\rangle$. By 5.169(REq), $t_2 = t_3$, and $\sigma_2 = \sigma_3$, and $\Sigma_2 = \Sigma_3$, and $\rho_2 = \rho_3$. Choose $\mathrm{F}_2 = \mathrm{F}_3$. □

**Lemma 5.176** (TP). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T$*, and* $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \longmapsto \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, then there exists* $\mathrm{F}_2$*, such that* $\mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle : T$*.*

*Proof.* Directly by 5.175(TPEq). □

**Lemma 5.177** (TPEqj). *If* $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \longmapsto^j \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, and* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T$*, then* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto^j \mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*.*

*Proof.* Induction on $j$:

- If $j = 1$. By 5.175(TPEq).
- Otherwise, $j > 1$, $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle \longmapsto \langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle$, and $\langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle \longmapsto^{j-1} \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$. By 5.175(TPEq), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_1, \mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle$. By induction, $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto^{j-1} \mathrm{F}_1, \mathrm{F}_3, \mathrm{F}_4 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$, and $\mathrm{F}_1, \mathrm{F}_3, \mathrm{F}_4 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle : T$. Choose $\mathrm{F}_2 = \mathrm{F}_3, \mathrm{F}_4$.

□

To prove the Immutability guarantee, we first in 5.178(MP) show that a reduction step does not make any existing objects mutably reachable, then in 5.179(MPP) extend this to an arbitrary number of steps. The theorem 5.180(TyIG) states the immutability guarantee for typed reduction, guaranteeing that a object which is not mutably reachable will not be modified. The theorem 5.181(IG) states the immutability guarantee for untyped reduction, shown from 5.180(TyIG) by ignoring the types.

**Theorem 5.178** (MP). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*,* $y \to d \in \Sigma_1$*, and* $\mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$ **mreach** $y$*, then* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$*.*

*Idea.* A typed reduction step does not make existing objects **mreach** if they weren't before. ▽

*Proof.* By cases on typed reduction:

- Case (TR-Apply): $t_1 = w_1.m\, w_2$, and $t_2 = [w_1/r][w_2/z]t$, and $\Sigma_2 = \Sigma_1$, and $\sigma_2 = \sigma_1$, and $\rho_2 = \rho_1$, and $\mathrm{F}_2 = \mathrm{F}_1$. By 5.150(MPApply), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$.
- Case (TR-Read): $t_1 = w_1.a$, and $t_2 = \mathsf{v}w_2$, and $\Sigma_2 = \Sigma_1$, and $\sigma_2 = \sigma_1$, and $\mathrm{F}_2 = \mathrm{F}_1, w_2 : T_2$. By 5.141(MPRead), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$.
- Case (TR-Write): $t_1 = w_1.a := w_3$, and $t_2 = \mathsf{v}w_3$, and $\sigma_2 = \sigma_1$, and $\rho_2 = \rho_1$, and $\mathrm{F}_2 = \mathrm{F}_1$. By 5.144(MPWrite), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$.
- Case (TR-LetNew): $t_1 = \mathsf{let}\ z = \nu(s : R)d\ \mathsf{in}\ t$, and $t_2 = [w_1/z]t$, and $\sigma_2 = \sigma_1$, and $\mathrm{F}_2 = \mathrm{F}_1, y_1 : T_1, w_1 : T_1$, and $\mathrm{F}_1;\rho_1 \sim \Sigma_1$. Because $y \to d \in \Sigma_1$, we have $y \in \mathrm{F}_1$. By 5.159(MPLetNew), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$.
- Case (TR-LetPush): $t_1 = \mathsf{let}\ z = t_3\ \mathsf{in}\ t_4$, and $t_2 = t_3$, and $\Sigma_2 = \Sigma_1$, and $\rho_2 = \rho_1$, and $\mathrm{F}_2 = \mathrm{F}_1$. By 5.163(MPLetPush), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$.
- Case (TR-LetLoc): $t_1 = \mathsf{v}w_1$, and $t_2 = [w_1/z]t_3$, and $\Sigma_2 = \Sigma_1$, and $\rho_2 = \rho_1$, and $\mathrm{F}_2 = \mathrm{F}_1$. By 5.168(MPLetLoc), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$.

□

**Theorem 5.179** (MPP). *If* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto^k \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*,* $y \to d \in \Sigma_1$*, and* $\mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$ **mreach** $y$*, then* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$*.*

*Idea.* Typed reduction does not make existing objects **mreach** if they weren't before. ▽

*Proof.* Induction on $k$. If $k = 0$, then trivially. Otherwise, there exists $\langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle$, such that $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto^{k-1} \mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle$, and $\mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle : T \longmapsto \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$. By 5.178(MP), $\mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3\rangle$ **mreach** $y$. By induction, $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$. □

**Theorem 5.180** (TyIG). *If* $y \to d \in \Sigma_1$*, and* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle : T \longmapsto^k \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2\rangle$*, then either* $y \to d \in \Sigma_2$ *or* $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$ **mreach** $y$*.*

*Idea.* If an object at location $y$ is changed during reduction, then it must be mutably reachable from the starting configuration. ▽

*Proof idea.* If an object $y$ is mutated in a step, then it must be mutably reachable. Because of **mreach** preservation, it must also be **mreach** in $\langle t_1; \sigma_1; \rho_1; \Sigma_1\rangle$. ▽

*Proof.* Induction on number of steps $k$ using 5.125(MMR) and 5.178(MP). If $k = 0$, then trivially $\Sigma_2 = \Sigma_1$. Otherwise, there exists $\langle t_3; \sigma_3; \rho_3; \Sigma_3 \rangle$, such that $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle : T \longmapsto^{k-1} \mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3 \rangle$, and $\mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3 \rangle : T \longmapsto \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2 \rangle$. By induction, either $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle$ $\mathbf{mreach}$ $y$, or $y \rightarrow d \in \Sigma_3$. In the second case. By 5.125(MMR), either $\mathrm{F}_3 \vdash \langle t_3; \sigma_3; \rho_3; \Sigma_3 \rangle$ $\mathbf{mreach}$ $y$, or $y \rightarrow d \in \Sigma_2$. In the first case. By 5.179(MPP), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle$ $\mathbf{mreach}$ $y$. □

**Theorem 5.181** (IG). *If $y \rightarrow d \in \Sigma_1$, and $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle : T$, and $\langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle \longmapsto^k \langle t_2; \sigma_2; \rho_2; \Sigma_2 \rangle$, then either $y \rightarrow d \in \Sigma_2$ or $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle$ $\mathbf{mreach}$ $y$.*

*Idea.* If an object at location $y$ is changed during reduction, then it must be mutably reachable from the starting configuration. ▽

*Proof idea.* By typed progress and preservation, show that typed reduction takes the same $j$ steps. Follows by 5.180(TyIG). ▽

*Proof.* By 5.177(TPEqj), $\mathrm{F}_1 \vdash \langle t_1; \sigma_1; \rho_1; \Sigma_1 \rangle : T \longmapsto^j \mathrm{F}_1, \mathrm{F}_2 \vdash \langle t_2; \sigma_2; \rho_2; \Sigma_2 \rangle$. By 5.180(TyIG). □

# References

[1] Vlastimil Dort and Ondřej Lhoták. Reference mutability for DOT. In preparation.

[2] Ifaz Kabir. $\kappa$DOT: A DOT calculus with mutation and constructors. Master's thesis, University of Waterloo, 2018.

[3] Ifaz Kabir and Ondřej Lhoták. $\kappa$DOT: scaling DOT with mutation and constructors. In *Proceedings of the 9th ACM SIGPLAN International Symposium on Scala, SCALA@ICFP 2018, St. Louis, MO, USA, September 28, 2018*, pages 40–50, 2018.

[4] Marianna Rapoport, Ifaz Kabir, Paul He, and Ondřej Lhoták. A simple soundness proof for dependent object types. *PACMPL*, 1(OOPSLA):46:1–46:27, 2017.